Encentuate® Identity and Access Management (IAM)

Helpdesk Guide

Product version 3.5

Document version 3.5.2

Copyright notice

Encentuate® IAM Helpdesk Guide version 3.5.2

NO WARRANTY: Any documentation made available to you is as is, and Encentuate makes no warranty of its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. Encentuate reserves the right to make changes without prior notice.

Trademarks

Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: http://support.encentuate.com/customerservice/

To reach us by phone:

- Singapore/Asia Pacific: +65-6471-1855
- USA: 1-800-ENCENTUATE

Table of Contents

About this guide

Welcome to the Encentuate IAM Helpdesk Guide.

Use this guide to provide Helpdesk services to users of Encentuate IAM Enterprise.

Purpose

This guide provides procedures to help users install and use Encentuate IAM Enterprise. It aims to cover the functionality and setup options of the product including internal implementation details (such as, describes what the product does and how to set it up).

Audience

The target users for this guide are Helpdesk officers supporting Encentuate AccessAgent, Encentuate AccessAssistant, and Encentuate AccessAdmin. We assume that you have intermediate computing knowledge, and are familiar with common computer and Windows-related terms.

What's in this guide

IAM Overview provides an introduction to the Encentuate Identity and Access Management Suite's features.

Helpdesk duties discusses the responsibilities of a Helpdesk officer.

Managing users discusses how to manage users using Encentuate AccessAdmin.

Managing user policies covers general procedures for managing user policies.

Viewing system policies discusses how system policies are viewed in AccessAdmin.

Troubleshooting discusses how to deal with the different problems you may encounter in connection with Encentuate AccessAgent, Encentuate Wallet, Encentuate password, or second authentication factors.

Document conventions

Refer to this section to understand the distinctions of formatted content in this guide.

Main interface elements

The following are highlighted in bold text in the guide: dialog boxes, tabs, panels, fields, checkboxes, radio buttons, fields, buttons, folder names, policy IDs/names, and keys. Examples are: **OK**, **Options** tab, and **Account Name** field.

Navigation

All content that helps users navigate around an interface is italicized (for example: *Start >> Run >> All Programs*)

Cross-references

Cross-references refer you to other topics in the guide that may provide additional information or reference. Cross-references are highlighted in green and display the referring topic's name (for example: Document conventions).

Hyperlinks

Hyperlinks refer you to external documents or web pages that may provide additional information or reference. Hyperlinks are highlighted in blue and display the actual location of the external document or web page (for example: http://www.encentuate.com).

Scripts, commands, and codes

Scripts, commands, or codes are those entered within the system itself for configuration or setup purposes, and are usually formatted in Courier font.

For example:

```
<script language="JavaScript">

<!--

  ht_basename = "index.php";

  ht_dirbase = "";

  ht_dirpath = "/" + ht_dirbase;

//-->

</script>
```

Tips or Hints

Tips or hints help explain useful information that would help perform certain tasks better.

Warnings

Warnings highlight critical information that would affect the main functionalities of the system or any data-related issues.

IAM Overview

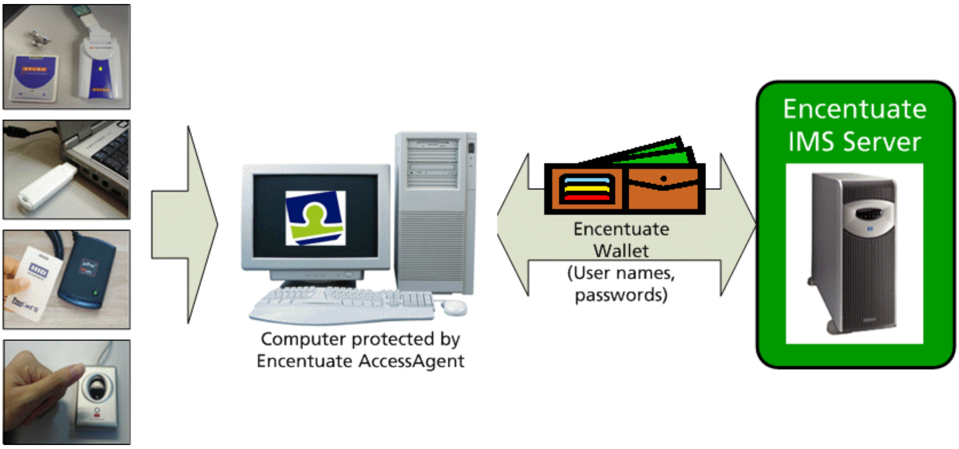
This chapter provides a brief overview of Encentuate IAM and its various components.

This chapter covers the following topics:

- Illustrated workflow
- Components of Encentuate IAM
- Authentication factors
- Understanding Encentuate icons

Illustrated workflow

The following diagram illustrates a simplified version of the Encentuate IAM workflow.



Encentuate IAM workflow

Components of Encentuate IAM

The main components of Encentuate IAM are:

- Encentuate Wallet
- Encentuate AccessAgent
- Encentuate AccessAdmin
- Encentuate AccessAssistant
- Encentuate AccessStudio
- Encentuate IMS Server
- Encentuate Web Workplace

To use Encentuate AccessAgent, set:

- Encentuate password
- Secret

The Encentuate password can be made stronger or replaced by a second "authentication factor". The combination of the password and a USB Key, for example, strengthens your computer's security because both authentication factors need to be present to access your computer.

Based on your organization's security policy, you may be required to use one of the following second authentication factors:

- Encentuate USB Key
- Encentuate USB Proximity Key
- Encentuate RFID card
- Encentuate Active Proximity Badge
- Encentuate Fingerprint Identification

Encentuate Wallet

The Encentuate Wallet stores the user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). The use of the Wallet is governed by a set of security policies. Each user has a Wallet, protected by a lock. The key to the lock can be as simple as an Encentuate password fortified with a second authentication factor.

The Wallet can be located at any point of access where an Encentuate AccessAgent is installed.

Cached Wallet

A “cached” Wallet is a copy of the user’s Wallet which is stored in the hard disk of the computer. The user can retrieve the cached Wallet during emergencies (for example, access without IMS Server connectivity.)

In an environment where computers are regularly shared by several users, a user may have access to several computers. In this scenario, caching a Wallet saves a lot of time for the user, and does not require regular downloaded of Wallet from the IMS server again for each use. The Wallet can also be cached in the computer.

Encentuate AccessAgent

Encentuate AccessAgent is the client software that manages the user’s Wallet, enabling automatic sign-on to applications and strong authentication.

Encentuate AccessAdmin

Encentuate AccessAdmin is the management console used by Administrators and Helpdesk officers to manage users and policies.

Encentuate AccessAssistant

Encentuate AccessAssistant is the web-based interface used to provide password self-help. AccessAssistant is used to obtain the latest credentials to log on to applications.

Encentuate AccessStudio

Encentuate AccessStudio enables an Administrator to create AccessProfile data and save it to a file. AccessProfiles and their associated data can also be downloaded and modify from either the Encentuate IMS Server or the local installation of AccessAgent.

Encentuate IMS Server

Encentuate IMS Server is responsible for identity management, certificate management, and recording administrative, user and system actions in audit logs.

A backup of the user’s Wallet’s contents is stored on the IMS Server, so AccessAgent can retrieve the backed-up information by connecting to the IMS Server with proper authentication. The information is encrypted and cannot be read by anyone, including Helpdesk officers and Administrators.

Encentuate Web Workplace

Encentuate Web Workplace is a Web-based interface that gives users the ability to log on to enterprise Web applications by clicking on hyperlinks, without specifying the password for each application. It can be integrated with the customer's existing portal or SSL VPN.

Authentication factors

Encentuate authentication factors come in different forms and functions. With the exception of password and fingerprint, users access systems and applications with a device that works like a key.

Encentuate password

The Encentuate password is used to secure access to an Encentuate Wallet. The user specifies a password upon signing up with Encentuate AccessAgent. Signing up with Encentuate AccessAgent means registering the user with the IMS Server, and creating an Encentuate Wallet.

If Microsoft Active Directory (AD) is used as the enterprise directory, the Encentuate password can synchronize with the Active Directory password. This means users can use the same Active Directory credentials to log on to Encentuate software. This option can be enabled during the Active Directory configuration.

Secret

The user is asked to enter a secret when signing up for an Encentuate Wallet. A secret is a second password or a backup password. It is similar to the "hint" provided when the user forgets the password for a Web e-mail account, for example. The secret should be something that:

- the user will not forget, even if it is not used it for a long time
- is not likely to change
- is known only to the user

When the user signs up, the user selects a Question from a list, and then provides the Answer to that question. If the Encentuate password is forgotten, the secret will help the user to set a new Encentuate password. The user can also use the secret, along with an authorization code, to gain temporary access to the Wallet. An authorization code is generated by a Helpdesk officer or an Administrator.

Second authentication factors

The Encentuate password can be fortified by a second authentication factor. The combination of the password and a USB Key, for example, strengthens the user's computer's security because both authentication factors must be present to access the computer.

Based on your organization's security policy, you may be required to use one of the following authentication factors.

Encentuate ActiveCode

The Encentuate ActiveCodes are short-term authentication codes that are controlled by the Encentuate IAM system.

There are two types of ActiveCodes:

- Mobile ActiveCode

  An Encentuate Mobile ActiveCode is a one-time password that is randomly generated and event-based. The Mobile ActiveCode is generated on the IMS Server and delivered via a secure second channel, such as text services (SMS) on mobile phones. It is used for strong authentication.

- Unified ActiveCode

  The Encentuate Unified ActiveCode is a predictive one-time password used for strong authentication. The Unified ActiveCode generator is built into AccessAgent. Software-only Clients will be available for: Windows, PocketPC, PalmOS, and Macintosh. A Unified ActiveCode can also be generated onboard by the Encentuate USB Key.

The use of ActiveCodes enhances the security of traditional password-based authentication for applications, since ActiveCodes are random passwords that can only be used once by an authorized user. Combined with alternative channels and devices, ActiveCodes provide effective second-factor authentication.

Encentuate USB Key

The Encentuate USB Key is a removable USB drive that combines the utility and storage capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) into one package. Encentuate's USB Key can store user names, passwords, certificates, encryption keys, and other security credentials.

Encentuate USB Proximity Key

The Encentuate USB Key can be equipped with RFID (Radio Frequency Identification), an electronic device that uses radio frequency signals to read identification information stored within. The USB Key with RFID integration is called the Encentuate USB Proximity Key.

Encentuate USB Key/USB Proximity Key

The USB Proximity Key requires a proximity reader to work. The proximity reader is installed on your computer use with Encentuate AccessAgent, or on any other hardware that requires authorization. For example, your office front door or elevator can have a proximity reader so that access is restricted to those with an RFID built into their Encentuate USB Key.

Encentuate RFID card

The Encentuate RFID card is an electronic device that uses radio frequency signals to read identification information stored within. Unlike the USB Proximity Key, the RFID card does not have any storage capacity.

Encentuate RFID card also allows for unified access - which means you can use it to access your computer, as well as for physical security (to access doors, elevators, etc.). The RFID card is also referred to the Building Access Badge.

Encentuate RFID card and reader

Encentuate Active Proximity Badge

The Encentuate Active Proximity Badge works in an almost identical way as the regular RFID Card - it has RFID, and works with a proximity reader. However, the Active Proximity Badge slightly differs in the range that it covers.

With the regular Encentuate RFID Card, the card needs to be in close proximity with the reader. With the Active Proximity Badge, the distance can be specified. For example, your Active Proximity Badge can be two meters away from the reader, yet it will be recognized.

Encentuate Active Proximity Badge and reader

Encentuate Fingerprint Identification

The Encentuate Fingerprint Identification system recognizes your fingerprint as an authentication factor. The fingerprint reader translates your fingerprint into encrypted codes, which in turn logs you on to AccessAgent on your computer.

Fingerprint reader

Presence detectors

A presence detector is a device that detects the presence of the user in its vicinity. If affixed to a computer, it can notify AccessAgent when someone comes in front of the computer or moves away.

Sonar device

The sonar-based presence detector is used to lock a workstation immediately when the user walks away without waiting for the desktop inactivity time-out. The device uses 40 kHz ultrasonic sound waves (frequency too high for people to hear). It can detect from a range of 5 inches to 5 feet. The user can move within the zone without triggering a walk-away event.

Sonar device

Active proximity badge

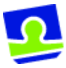
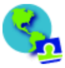
Active Proximity Badge is both a second factor authentication, as well as a presence detector as it is able to detect the presence of the user and AccessAgent can be configured to perform appropriate actions.

Refer to the recommended policy settings for using Active Proximity Badge as a presence detector.

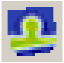
✓ *The presence detector policies (for example, pid_presence_detector_enabled) are not applicable to Active Proximity Badge.*

Understanding Encentuate icons

Application icons

Icon	Description
	This icon represents Encentuate AccessAgent application on the desktop.
	This icon represents Encentuate IMS Server on the desktop.

Notification area icons

Icon	Description
	No user has logged on to AccessAgent.
	AccessAgent is operating normally.

Helpdesk duties

This chapter discusses the duties of a Helpdesk officer.

This chapter covers the following topics:

- Confirming end-user identity
- Managing users and authentication factors
- Promoting good security practices

Confirming end-user identity

As a Helpdesk officer, you may receive requests from users to troubleshoot problems related to Encentuate AccessAgent, Encentuate Wallet, Encentuate password, or a second authentication factor. You may also need to issue a new second authentication factor, or provide an authorization code.

Always verify the user's identity to prevent unauthorized access to protected systems. You may communicate with the user personally, online, or over the telephone. Set a standard method of verifying the user's identity in line with your corporate policies.

You may require a user to provide information, such as employee number, Social Security number, or mother's maiden name. You should be able to verify the accuracy of these information.

A user may acquire the identity of a co-worker to gain unauthorized access. If you are suspicious, require more information. If cases of possible fraud, it should be dealt with according to the policies of your company.

Managing users and authentication factors

As a Helpdesk officer, you are responsible for managing users and authentication factors. You should be familiar with the different user processes and troubleshoot problems, such as the inability to install Encentuate AccessAgent, logon failures, forgotten passwords, or loss of second authentication factors.

To learn more about the system, go through the Encentuate IAM User Guide and familiarize yourself with processes, such as installation, logon, or password modification. A solid understanding of the contents of the Encentuate IAM User Guide will help you to accurately refer users to the appropriate solutions.

As an Encentuate Helpdesk officer, you are responsible for handling second authentication factors. Some responsibilities include distribution, maintenance, and safekeeping.

Managing users

- Help with forgotten passwords

  See Forgotten password in Troubleshooting.

- Deprovisioning separated employees

  When an employee leaves the organization, you must revoke the user's Wallet and second authentication factor. You may also need to revoke a second authentication factor if it has been reported lost or stolen.

  Revocation is permanent within the Encentuate system. Once a second authentication factor is revoked, it cannot be re-used unless it is re-registered. If the second authentication factor is a USB Key, it has to be reset before if can be re-registered.

  See Revoking a second authentication factor.

✓	*Revocation is permanent only within the Encentuate system. In revoking access cards, the system does not integrate with other infrastructure management systems such as Kronos.*

Managing second authentication factors

■ Providing second authentication factors to new employees

Orient each new employee on the basic concepts of Encentuate IAM and provide the person a copy of the Quick Start Guide. The Quick Start Guide provides basic instructions to help new users get started.

You may also need to provide a second authentication factor if your organization requires employees to use two-factor authentication. If applicable, stress that the second authentication factor should be kept safe, and a strong password should be used.

Initially, the user needs to sign up with a second authentication factor. After the user signs up, you can then search for the user and access information on the user's profile and the second authentication factor.

■ Replacing lost second authentication factors

The second authentication factor must be revoked once it is lost or stolen, to prevent unauthorized use. Note that revocation is permanent.

See Lost Encentuate USB Key, Lost Encentuate RFID card, or Lost Encentuate Active Proximity Badge in Troubleshooting.

■ Replacing a locked Encentuate USB Key

The Encentuate USB Key is locked after a preset number of attempts to log on using an incorrect password. A locked Encentuate USB Key cannot be used, until it is reset. If a USB Key is locked, provide the user with a new USB Key.

A locked USB Key must be sent to Encentuate for reprogramming.

■ Safeguarding unused second authentication factors

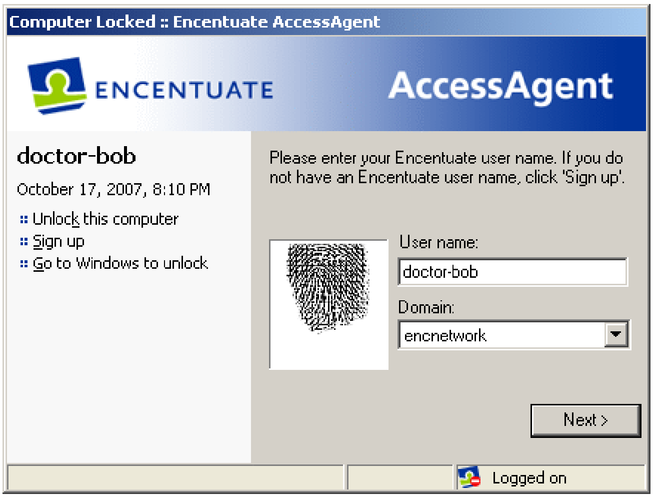
Unused second authentication factors must be kept in a dry and secure place with restricted access. If there are two or more Helpdesk officers in your organization, only one should be designated to monitor the inventory. A contingency plan should be set in case the designated officer is unavailable.

Although second authentication factors are of no value either without user credentials, or unless registered with the IMS Server, these items should still be safeguarded like any other company resource. It is the responsibility of the designated Helpdesk officer to ensure that there is enough inventory for distribution to new employees or replacement of locked, lost, or damaged units.

Registering another finger under the same user

Sometimes, the finger or fingerprint of a user is unusable (for example, due to injury). In this case, you may have to register another finger, depending on the policies of your organization. Use AccessAgent to register another finger.

The first step is to lock the computer and place the finger to register on the fingerprint reader. Enter your user name and click **Next**.


Computer Locked :: Encentuate AccessAgent

doctor-bob

October 17, 2007, 8:10 PM

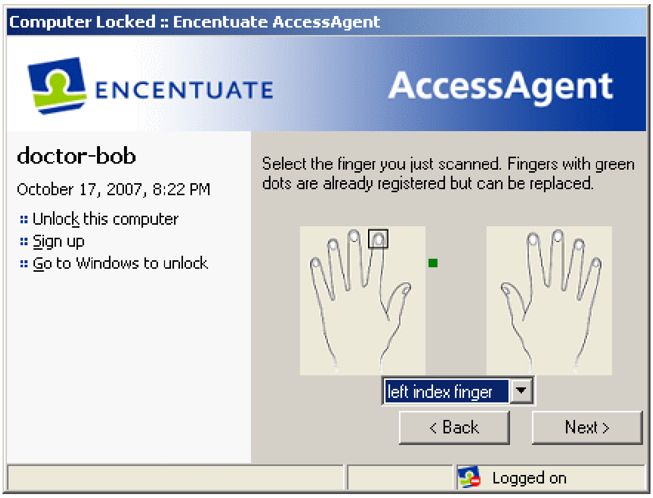
Please enter your Encentuate user name. If you do not have an Encentuate user name, click 'Sign up'.

User name: doctor-bob

Domain: encnetwork

Click **Register Fingerprint**. Enter your username and password and click **OK**.

Select the finger to register and then click **Next**.


Computer Locked :: Encentuate AccessAgent

doctor-bob

October 17, 2007, 8:22 PM

Select the finger you just scanned. Fingers with green dots are already registered but can be replaced.

left index finger

AccessAgent requires a finger to be scanned five times to complete registration.

Promoting good security practices

As a Helpdesk officer, advise users on how to protect their data from unauthorized access. The following are some of the most useful security practices.

- Choose strong passwords and keep them secure

  Dictionary words, names of family members and pets, and important dates do not make good passwords. Sophisticated software can generate millions of character combinations per second. At this rate, a weak password can be compromised in less than a minute.

  Advise users to choose passwords that are not easy to crack. A strong password is longer and combines upper and lowercase letters, numbers, and special characters.

The required length of passwords can be configured by the Administrator. For example, a minimum of eight characters and a maximum of 12 characters can be set. The Administrator can also configure the maximum number of attempts to log on using an incorrect password before the Encentuate Wallet is locked.

- Do not forget the secret

  Advise users to always remember their secrets. If Encentuate passwords are forgotten, secrets will help users to set new passwords.

  See Secret for more information.

- Safeguard the second authentication factor

  The second authentication factor fortifies the Wallet, and should be kept in a secure place. Use the following guidelines when advising users on safeguarding second authentication factors:

  - A second authentication factor should be treated like a key to your car or house. The information stored on the second authentication factor is personal and confidential. Only you should have access to it.

  - When leaving your workstation, take your second authentication factor with you or keep it in a secure place. If you leave it unguarded, someone else can log on to an enterprise application using your user name and password. That person can modify, copy, or delete confidential and important files, and you may be held liable for the unauthorized action.

- Safeguard the desktop

  Use the following guidelines when advising users on safeguarding their desktops:

  - If you are leaving your workstation, use the **Lock Computer** option that you can access by right-clicking on the Encentuate AccessAgent icon in the notification area. Alternatively, you can log off from AccessAgent or Windows. This allows another user to use your computer, if you are working on a shared workstation.

  - If another user will use your computer (even for only a few minutes), always log off your Encentuate Wallet.

- Report loss of a second authentication factor

  Advise users to inform Helpdesk if their second authentication factor is missing or misplaced. A stolen second authentication factor is not a high security risk, since the Encentuate password is still required. It would be difficult to obtain both the second authentication factor and the password at the same time to gain access. However, to avoid fraudulent use of a second authentication factor, Helpdesk officers must be informed of any loss immediately.

!	*Once a user reports a missing second authentication factor, revoke the second authentication factor immediately. For more information, see Revoking a second authentication factor.*

Managing users

This section discusses how to manage users with Encentuate AccessAdmin. You can access the Encentuate AccessAdmin user interface by going to the console of the machine where the IMS Server is installed. When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com.), and a logon prompt will be presented.

If the IMS server is accessed without using the fully qualified domain name, AccessAgent cannot automatically perform an SCR (logon) to the search page.

In the main user interface, you can find links to all the available administration functions. The main link, AccessAdmin, should be visible at all times. Click on the link to view the AccessAdmin user interface.

This chapter covers the following topics:

- Searching for a user
- Viewing a user's settings

Searching for a user

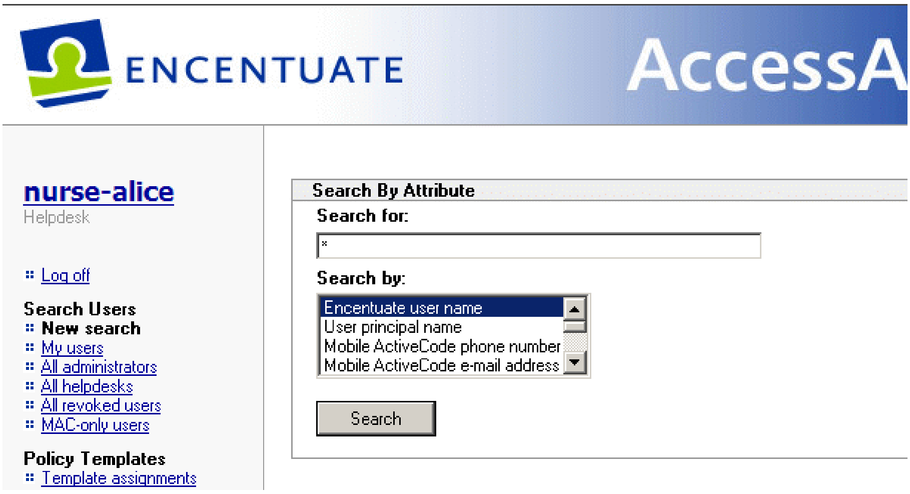
There are many ways you can search for users in AccessAdmin. You can search for a single user, a group of users, or users that have been assigned to you.

To search for a user:

❶ Click on *AccessAdmin >> Search Users >> New search*.

❷ Enter the subject of your search in **Search for**.

You can make a partial search and end the string with an asterisk (*). For example, if you want to find all users whose enterprise user name begins with the letter "i", enter "i" in the Search for field.*



Search By Attribute

Search for: *

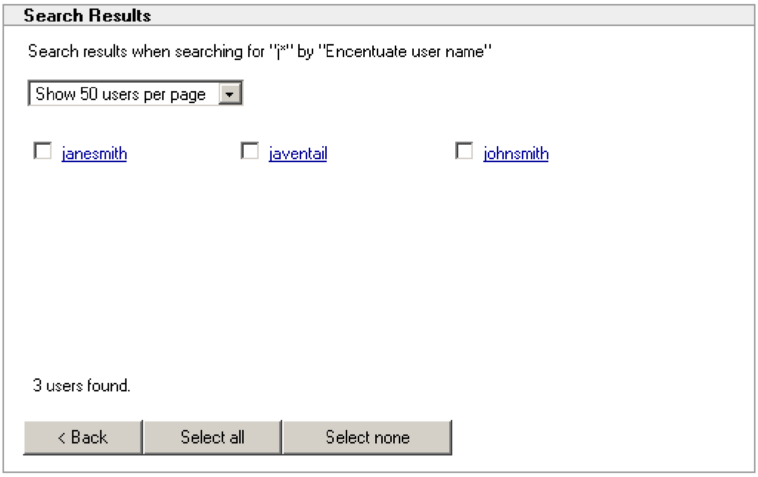
Search by:
- Encentuate user name
- User principal name
- Mobile ActiveCode phone number
- Mobile ActiveCode e-mail address

New search

❸ Select a search criteria from the **Search by** list.

❹ Click **Search**. The search results are displayed, containing all the matches or partial matches. You can also use partial name search—for example, if you want to find all users whose names start with the letter A, you can type **A*** in the **Search for** field. The matching result will appear on the screen.

Refine your search by marking the checkbox next to the corresponding user if the result is not comprehensive enough. Click on each matching user to view the user's settings.



Search Results

Search results when searching for "j*" by "Encentuate user name"

Show 50 users per page

□ janesmith □ javentail □ johnsmith

3 users found.

Search results

Newly registered Helpdesk officers are not automatically given the charge of all users. As such, if a user is not assigned to a Helpdesk, a search for this user by this Helpdesk may result in an empty set. The Helpdesk should refer this case to the Administrator who can assign the user to the Helpdesk.

Searching for a group of users (My users)

To search for a group of users (My users)

❶ Click on *AccessAdmin >> Search users >> My users*.

You can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list. Select one or more users by marking on the checkbox(es) next to the corresponding user(s).*

❷ View or modify the details for the particular user(s).

Searching for a group of users (MAC-only users)

Use this search to find users with Mobile ActiveCode (MAC) as their authentication method.

To search for a group of users (MAC-only users):

❶ Click on *AccessAdmin >> Search users >> MAC-only users*.

You can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list. Select one or more users by marking on the checkbox(es) next to the corresponding user(s).*

❷ View or modify the details for the particular user(s).

Viewing a user's settings

To view a user's settings:

❶ Search for a user. See Searching for a user.

❷ The user's settings will show the following information:

- The user's Audit logs

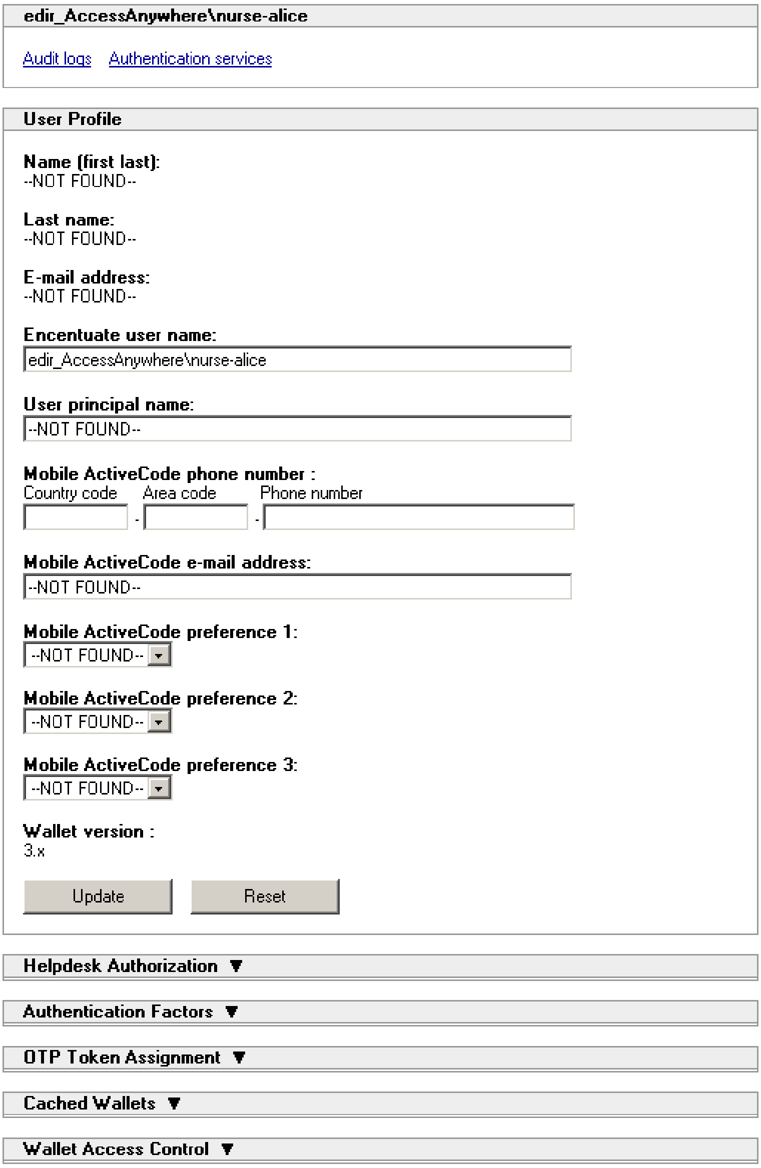
  These are the user activity logs, which record the time of the activity, the type of activity, and the achieved result.

- Authentication services

  These are the types of user’s certificate-enabled, enterprise and personal authentication services, which appears as a link at the top of the page.

You can also view the following user’s attributes:

- Personal data (e.g., name, email address, Encentuate user name, etc.)
- Mobile ActiveCode preferences (if any)
- Helpdesk authorization panel, for issuance of authorization codes
- Authentication factors of the user, their serial numbers and types
- All cached Wallets and their locations
- The Wallet access control status (available/not available)
- USB Key reset privilege
- Authentication, administrative, password, Wallet, and AccessAgent policies



edir_AccessAnywhere\nurse-alice

Audit logs Authentication services

User Profile

Name (first last):
--NOT FOUND--

Last name:
--NOT FOUND--

E-mail address:
--NOT FOUND--

Encentuate user name:
edir_AccessAnywhere\nurse-alice

User principal name:
--NOT FOUND--

Mobile ActiveCode phone number :
Country code - Area code - Phone number

Mobile ActiveCode e-mail address:
--NOT FOUND--

Mobile ActiveCode preference 1:
--NOT FOUND--

Mobile ActiveCode preference 2:
--NOT FOUND--

Mobile ActiveCode preference 3:
--NOT FOUND--

Wallet version :
3.x

User's settings

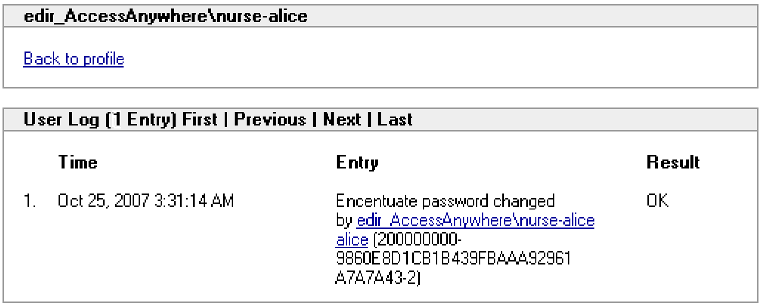
Viewing a user's audit logs

Use audit logs to view a listing of all user actions.

To view a user's audit logs:

❶ Search for one user. See Searching for a user.

❷ When you see the user's settings, click **Audit logs**. The system displays the user's log entries.



edir_AccessAnywhere\nurse-alice

Back to profile

User Log (1 Entry) First | Previous | Next | Last

	Time	Entry	Result
1.	Oct 25, 2007 3:31:14 AM	Encentuate password changed by edir_AccessAnywhere\nurse-alice alice (200000000-9860E8D1CB1B439FBAAA92961A7A43-2)	OK

View user's audit logs

Viewing a user's authentication services

When a user logs on to authentication services using an Encentuate Wallet, the information synchronizes with the Encentuate IMS Server via AccessAgent. Encentuate AccessAgent aggregates identities, stores them in the Wallet, and synchronizes it with Encentuate IMS Server.

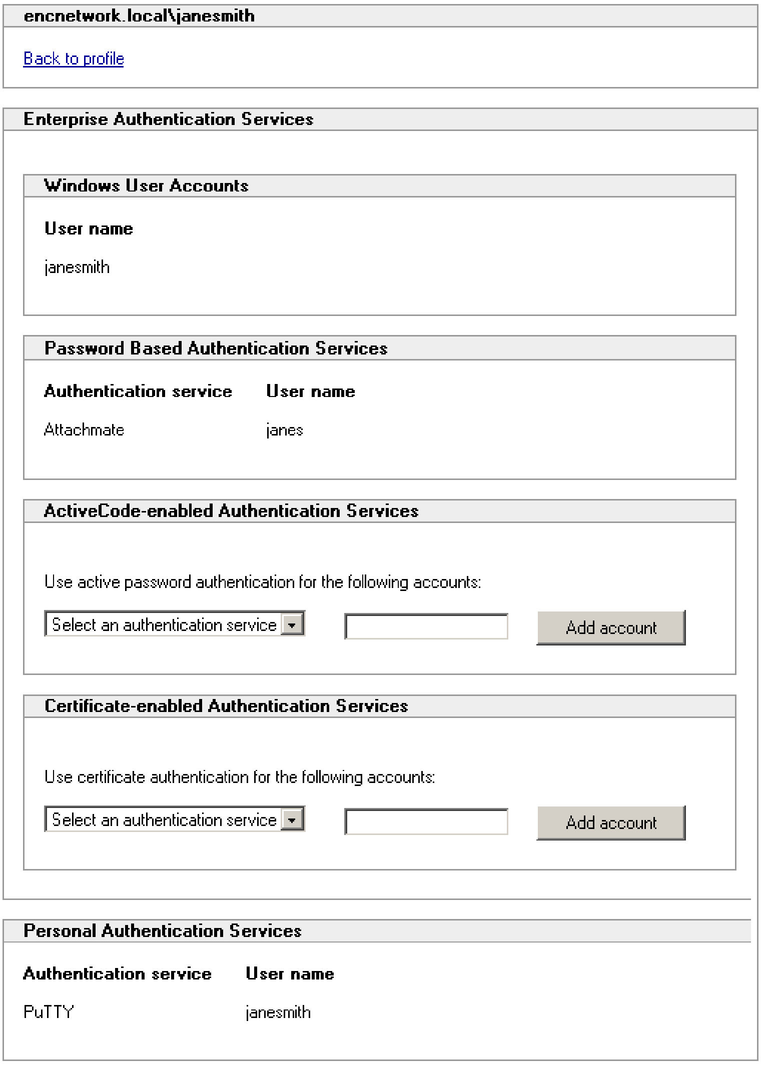
You can search for a user and view consolidated listings of a user's authentication services.

To view a user's authentication services, search for a user or select one from **My users**. Click **Authentication service**.

To view a user's authentication services:

❶ Search for a user. See Searching for a user.

❷ When you see the user's settings, click **Authentication services**. The system displays the user's authentication services.



encnetwork.local\janesmith

Back to profile

Enterprise Authentication Services

Windows User Accounts

User name

janesmith

Password Based Authentication Services

Authentication service	User name
Attachmate	janes

ActiveCode-enabled Authentication Services

Use active password authentication for the following accounts:

Certificate-enabled Authentication Services

Use certificate authentication for the following accounts:

Personal Authentication Services

Authentication service	User name
PuTTY	janesmith

Select an authentication service
Add account
Select an authentication service
Add account

User's authentication services

If the organization will not use Encentuate Wallets with personal authentication services, the system will not display any entries under personal authentication services.

Adding a user to a certificate-enabled authentication service

When an authentication service is certificate-enabled, you can add a user to the authentication service. This allows users to log on to the certificate-enabled authentication service without entering a user name and password.

To add a user to a certificate-enabled authentication service:

1. Search for a user. See Searching for a user.
2. In the user's settings, click **Authentication services**.
3. Scroll down to **Certificate-enabled Authentication Services**. From the drop-down list, select the certificate-enabled authentication service that will have a new user.
4. Enter the user's user name for the certificate-enabled authentication service.
5. Click **Add account**.

   The certificate-enabled authentication service, along with the user name, will be added.

Removing a user from a certificate-enabled authentication service

When disabling certificates for a user, use either of the options in the **Status** drop-down list.

To remove a user from a certificate-enabled authentication service:

1. Search for a user. See Searching for a user.
2. In the user's settings, click **Authentication services**.
3. Scroll down to **Certificate-enabled Authentication Services**.
4. From the drop-down list, select the user name to delete for a certificate-enabled authentication service.
5. Click **Delete account**.

   The user is now disabled from the certificate-enabled authentication service.

Editing a user's settings or attributes

To edit a user's settings or attributes, make the necessary changes to the enabled fields. View-only fields are greyed out. Click **Update** to confirm the changes.

Generating authorization codes

The authorization code is a random alphanumeric code that is required to retrieve credentials. The authorization code is *not* case-sensitive, so you can omit the hyphens and capitalization.

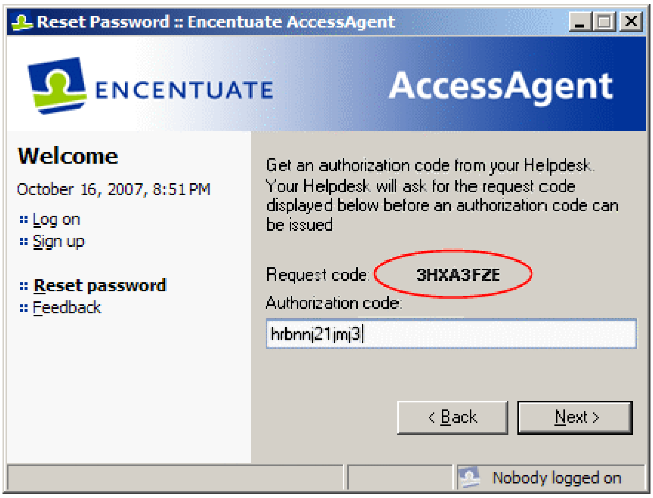
Every time you generate a new authorization code, the previous authorization code is replaced.

An authorization code is necessary if:

- The user forgot the Encentuate password
- The user lost the second authentication factor

To generate an authorization code:

1. Search for a user. See Searching for a user.
2. Ask the user whether a request code is shown on the user's screen.



Get an authorization code from your Helpdesk. Your Helpdesk will ask for the request code displayed below before an authorization code can be issued

Request code: 3HXA3FZE

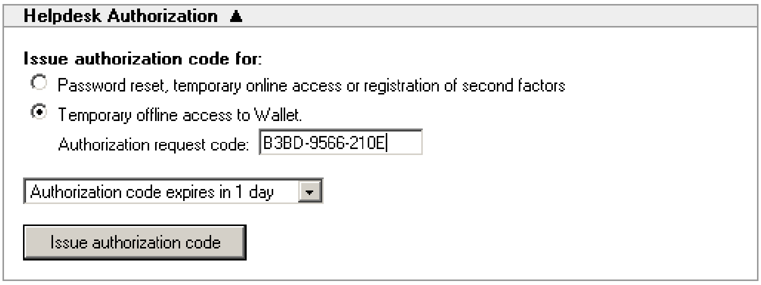
Authorization code: hrbnnj21jmj3

User's AccessAgent window - Request code

- If a request code is displayed, mark the **Temporary offline access to Wallet** radio button in the Helpdesk Authorization panel, and enter the request code.

A request code may have been provided to the user during connectivity issues with the IMS server. As a security measure, the user must provide a request code before issuing an authorization code for temporary offline access.

Inform the user that for temporary offline access, the new password is only valid for the user's current computer.



Helpdesk Authorization ▲

Issue authorization code for:

○ Password reset, temporary online access or registration of second factors

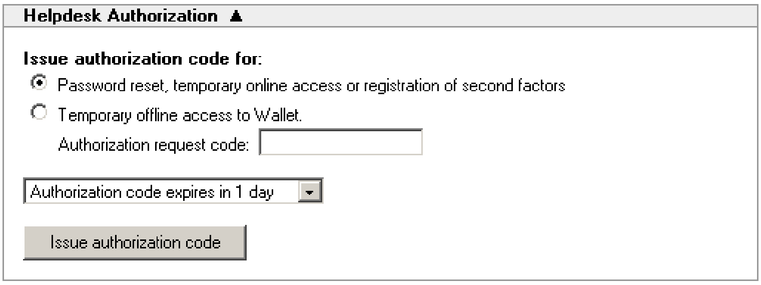
● Temporary offline access to Wallet.

Authorization request code: B3BD-9566-210E

Authorization code expires in 1 day ▾

Temporary offline access

- If there is NO request code, mark the **Password reset, temporary online access or registration of second factors** radio button in the Helpdesk Authorization panel.



Helpdesk Authorization ▲

Issue authorization code for:

● Password reset, temporary online access or registration of second factors

○ Temporary offline access to Wallet.

Authorization request code:

Authorization code expires in 1 day ▾

Password reset, temporary online access, or registration of second factors

❸ If applicable, enter the **Request Code** given by the user. This code is *not* case-sensitive.

❹ Select a validity period from the options in the drop-down list.

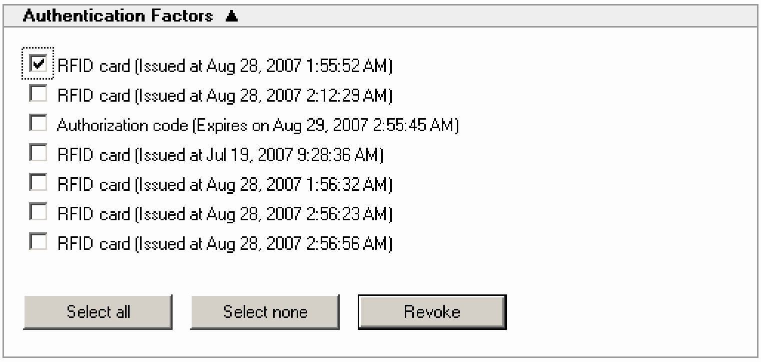
❺ Click **Issue authorization code**.

An authorization code appears on your screen and can now be relayed to the user. Mention that the authorization code should be used immediately.

After the user has registered a second authorization factor with the authorization code, the authentication factor's information synchronizes with Encentuate IMS Server and will be displayed under the user's settings.

Viewing a user's authentication factors

When users sign up for a new Encentuate Wallet or registers a second authentication factor, the information synchronizes with the IMS Server. An entry with the corresponding second authentication factor is added under the user's settings. Once completed, you can view the user's second authentication factor (s).



Authentication Factors ▲

☑ RFID card (Issued at Aug 28, 2007 1:55:52 AM)
□ RFID card (Issued at Aug 28, 2007 2:12:29 AM)
□ Authorization code (Expires on Aug 29, 2007 2:55:45 AM)
□ RFID card (Issued at Jul 19, 2007 9:28:36 AM)
□ RFID card (Issued at Aug 28, 2007 1:56:32 AM)
□ RFID card (Issued at Aug 28, 2007 2:56:23 AM)
□ RFID card (Issued at Aug 28, 2007 2:56:56 AM)

Registered second authentication factors

Revoking a second authentication factor

You may need to revoke a second authentication factor when it is reported lost or stolen.

To revoke a second authentication factor:

❶ Search for the user whose second authentication factor you want to revoke. See Searching for a user.

❷ In the user's settings, scroll down to the **Authentication Factors** panel. The user's authentication factors are displayed. Mark the checkbox of the authentication factor to revoke.

❸ Click **Revoke**.

Revoking a Wallet

Revoking a Wallet will prevent the user from logging on to the Wallet only on the specific computer where it is cached. Revoking a Wallet will not delete all references to the Wallet from the entire system.

When a user leaves the organization permanently, delete or revoke the user. If a user goes on leave for an extended period of time, lock the user's Wallet.

Locking and unlocking a Wallet

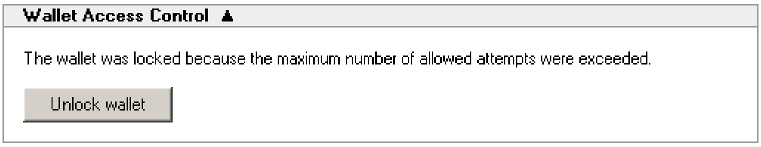
When a user attempts to log on using the wrong password and exceeds the maximum number of attempts allowed, the system will lock the Wallet. To unlock the Wallet, the user must contact the Helpdesk or Administrator to unlock the Wallet.

You can also lock a Wallet for the following reasons:

- To temporarily bar access to the user's Wallet (for example, when the user goes for an extended holiday).
- To prevent access until the user is deprovisioned or revoked from the IMS server (for example, when an employee leaves the organization).

To lock/unlock a Wallet:

1. Search for the user whose Wallet you want to lock/unlock. See Searching for a user.



Wallet Access Control ▲

The wallet was locked because the maximum number of allowed attempts were exceeded.

Locking or unlocking the Wallet

2. Click **Lock wallet** or **Unlock wallet** depending on the current status of the user's Wallet.

Signing up MAC-only users

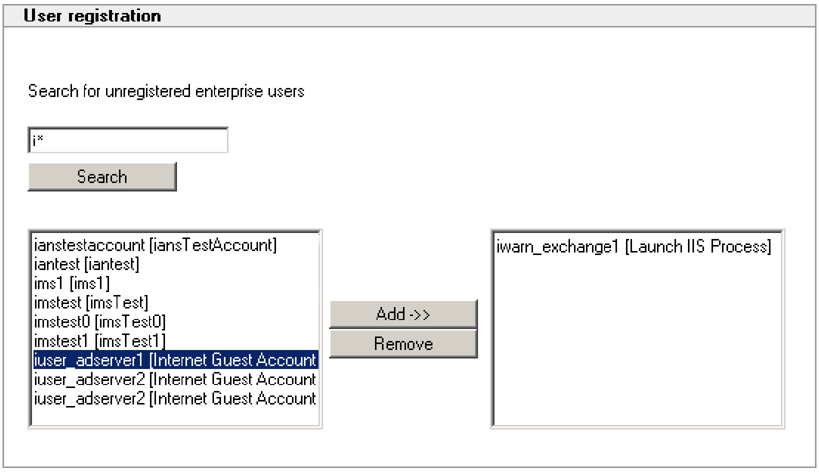
You can pre-provision enterprise users for MAC-only authentication, because they do not need an Encentuate password.

To sign up MAC-only users:

❶ In the AccessAdmin navigation panel, select *System >> User registration*.

❷ Search for an unregistered enterprise users by entering the user name and clicking **Search**.

✓ *Make a partial search by entering a keyword followed by an asterisk (*). For example, to find all users whose enterprise user names begin with the letter "i", enter "i*" in the Search for unregistered enterprise users field.*



User registration

Search for unregistered enterprise users

i*

ianstestaccount [iansTestAccount]
iantest [iantest]
ims1 [ims1]
imstest [imsTest]
imstest0 [imsTest0]
imstest1 [imsTest1]
iuser_adserver1 [Internet Guest Account
iuser_adserver2 [Internet Guest Account
iuser_adserver2 [Internet Guest Account

iwam_exchange1 [Launch IIS Process]

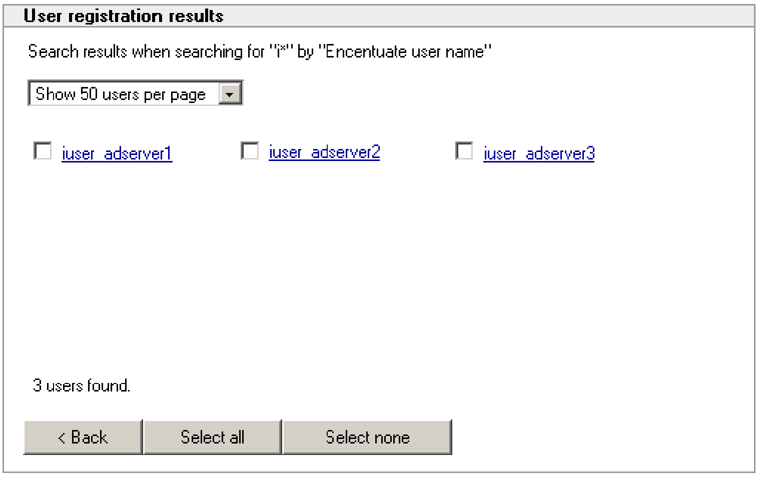
User registration

❸ When the unregistered enterprise user(s) appears in the Search Results panel, select a user by clicking on the user name. Select several users using the **Shift+click** or **Ctrl+click** keys.

❹ Click **Add** to move the users to the Selected Users panel. To remove users from the panel, click on the user name and then click **Remove**.

❺ Click **Add users**.

❻ If user registration is successful, the **User registration results** page lists all newly-provisioned users.



Search results when searching for "i*" by "Encentuate user name"

□ iuser_adserver1 □ iuser_adserver2 □ iuser_adserver3

3 users found.

User registration results

❼ To apply policies to new users, select a policy from the **Use policies from** drop-down list.

❽ Click **Update all**.

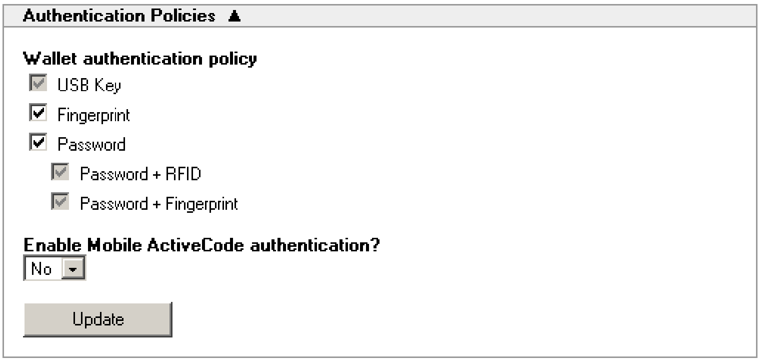
Managing user policies

This chapter discusses how to manage user policies using Encentuate AccessAdmin. You can access the Encentuate AccessAdmin user interface by going to the console of the machine where the IMS Server is installed. When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com.), and a logon prompt will be presented.

If the IMS server is accessed without using the fully qualified domain name, AccessAgent cannot automatically perform an SCR (logon) to the search page.

This chapter covers the following topics:

Setting Wallet authentication policies



Authentication Policies ▲

Wallet authentication policy

- ☑ USB Key
- ☑ Fingerprint
- ☑ Password
  - ☑ Password + RFID
  - ☑ Password + Fingerprint

Enable Mobile ActiveCode authentication?

No ▾

Wallet authentication policy

Use Authentication Policies to set Wallet authentication policies. The policies enforce the combinations of authentication factors that can be used for logging on. Mark the corresponding checkbox(es) to select an authentication factor, or use the drop-down list to modify a policy.

- Wallet authentication policy

  - USB Key

    Mark this option if a USB Key password is required.

  - Fingerprint

    Mark this option if fingerprint authentication is required.

  - Password

    Mark this option if two sub-policies are enabled. You can then modify the sub-policies as required.

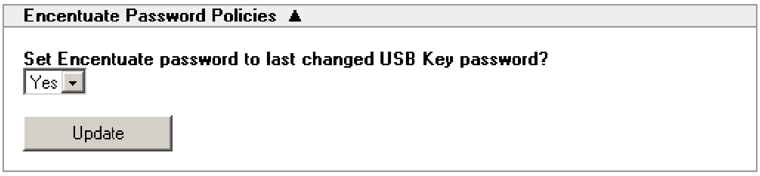
The option Password+RFID also includes the Active Proximity Badge.

- Enable Mobile ActiveCode authentication?

  Enable this policy if the user can authenticate using Encentuate Mobile ActiveCode.

Click **Update** to confirm the changes.

Setting Encentuate password policies



Encentuate Password Policies ▲

Set Encentuate password to last changed USB Key password?

Yes ▾

Password policies

- Set the Encentuate password to the last-changed USB Key password?

  The Encentuate password is different from the USB Key password. The USB Key's smart card is protected by its own password, which needs to synchronize with the Encentuate password.

  Set the policy to **Yes** for users who have one USB Key.

  Set the policy to **No** for users who have more than one USB Key.

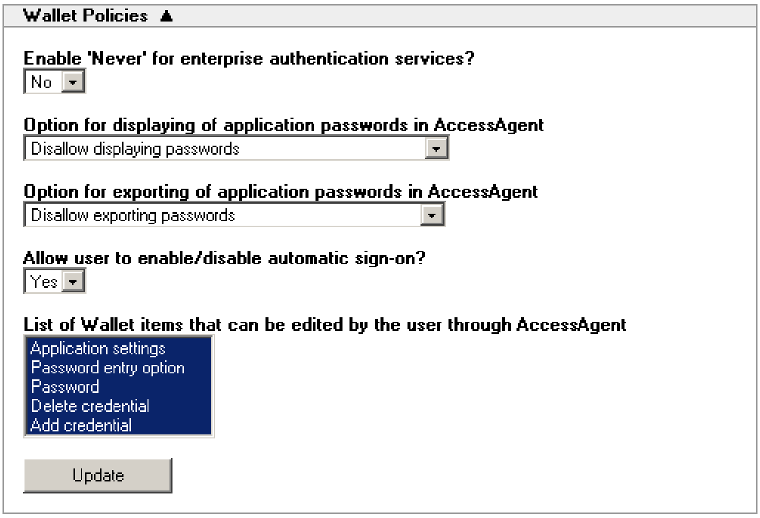
- **Force pre-provisioned user to change the Encentuate password at first logon**

  In some deployment scenarios, the user is pre-provisioned by a Helpdesk or an Administrator. This means that the Encentuate password is known to people other than the assigned user. Set the policy to **Yes** to make sure the user changes the Encentuate password after logging on for the first time.

Use the drop-down lists to modify the policies.

Click **Update** to confirm the changes.

Setting Wallet policies



Wallet Policies ▲

Enable 'Never' for enterprise authentication services?
No

Option for displaying of application passwords in AccessAgent
Disallow displaying passwords

Option for exporting of application passwords in AccessAgent
Disallow exporting passwords

Allow user to enable/disable automatic sign-on?
Yes

List of Wallet items that can be edited by the user through AccessAgent
Application settings
Password entry option
Password
Delete credential
Add credential

Wallet policies

Use this policies to set Wallet behaviors.

- **Enable "Never" for enterprise authentication services?**

  Set the policy to **Yes** if a user can set an enterprise authentication services' password entry option to **Never**.

  Set the policy to **No** if the password entry option will not have the option **Never**.

- **Option for displaying of application passwords in AccessAgent**

  Specify whether to display application passwords in the Wallet Manager of AccessAgent through the **Show passwords** option.

- **Option for exporting of application passwords in AccessAgent**

  Specify whether to export application passwords in the Wallet Manager of AccessAgent through the **Export?** option.

- **Allow user to enable/disable automatic signon?**

  Set **Yes** to allow the user to enable automatic signon. Set to **No** to disable automatic logon.

- **List of Wallet items that can be edited by the user through AccessAgent**

  Highlight each Wallet item that the user can edit through AccessAgent.

Encentuate recommends using the system default.

Click **Update** to confirm the changes.

Setting AccessAgent policies

Use AccessAdmin to manage all the policies that define AccessAgent's behavioral patterns on a computer when a user is logged on. The AccessAgent policies cover the following behavioral patterns:

- Desktop inactivity policies
- Lock/Unlock policies
- Second authentication factor-related policies
- Logon/logoff policies

Desktop inactivity policies

Use these policies to set locking and unlocking actions during desktop inactivity.

- **Policy priority for desktop inactivity**

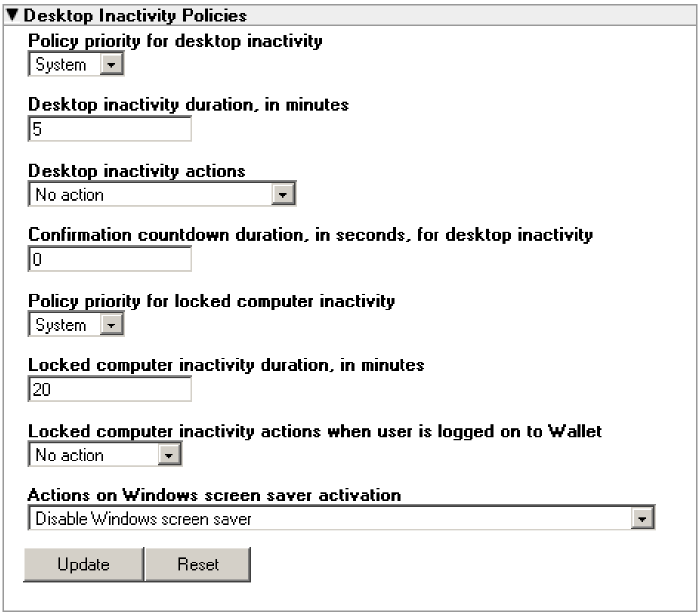
  Specify whether the system or machine policy should be enforced for desktop inactivity.

- **Desktop inactivity duration, in minutes**

  Enter the number of minutes the desktop is inactive before AccessAgent can perform a set of actions.

- Desktop inactivity actions

  Select the AccessAgent actions to be performed after a period of desktop inactivity.



▼ Desktop Inactivity Policies

Policy priority for desktop inactivity
System

Desktop inactivity duration, in minutes
5

Desktop inactivity actions
No action

Confirmation countdown duration, in seconds, for desktop inactivity
0

Policy priority for locked computer inactivity
System

Locked computer inactivity duration, in minutes
20

Locked computer inactivity actions when user is logged on to Wallet
No action

Actions on Windows screen saver activation
Disable Windows screen saver

Desktop inactivity policies

- Confirmation countdown duration, in seconds, for desktop inactivity

  Enter the number of seconds that AccessAgent will display a message box, which appears when AccessAgent is about to perform an action after a period of desktop inactivity.

  The message box provides two options for the user, one of which must be selected before the specified number of seconds expires. The user can either click Yes to let AccessAgent proceed with the action, or No to reactivate the desktop.

- Policy priority for locked computer inactivity

  Specify whether the system or machine policy should be enforced for locked computer inactivity.

- Locked computer inactivity duration, in minutes

  Enter the number of minutes of desktop inactivity, after which AccessAgent performs an action (for example, lock the computer).

- Locked computer inactivity actions when user is logged on to the Wallet

  Select the action that AccessAgent performs when desktop inactivity time has exceeded the specified limit.

- Actions on Windows screen saver activation

  If the computer uses the Windows screen saver, select the action that AccessAgent will perform when the Windows screen saver is activated.

Click Update to confirm the changes.

Lock/Unlock policies

Use these policies to specify lock/unlock conditions. Examples of policies include a logon script for auto-launching and a logoff script for clean-up operations, if any, after logging off from AccessAgent. These logon and logoff scripts should be included in the policy template.

- Enable lock script during locking of the user's AccessAgent session?

  Select Yes to run a lock script when locking a user's AccessAgent session.

- Lock script type

  Select the type of lock script to run when locking a session.

- Lock script code

  Enter the source code of the lock script to run when locking a session.

- Enable unlock script when user unlocks an existing AccessAgent session?

  Select Yes to run an unlock script when unlocking a user's existing AccessAgent session.

- Unlock script type

  Select the type of unlock script to run when unlocking a session.

- Unlock script code

  Enter the source code of the unlock script to run when unlocking a session.

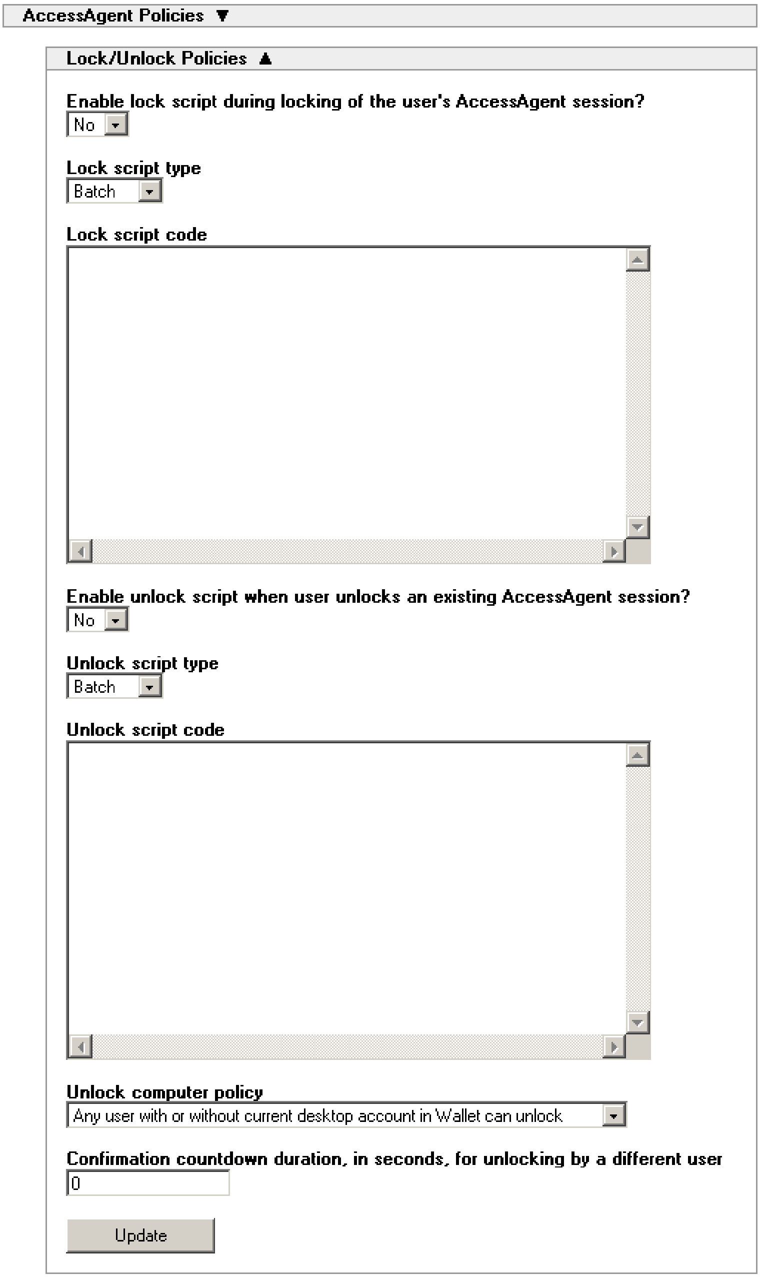
- Unlock computer policy

  Select the type of user allowed to unlock a computer after a logged on user has been locked. Same user refers to the user who locked the computer. Admin refers to the Windows user with Administrator privileges on the computer.

- Confirmation countdown, in seconds, for unlocking by a different user

  Specify the number of seconds a different user can unlock the computer. Enter 0 to disable this feature.

Click **Update** to confirm the changes.



AccessAgent Policies ▼

Lock/Unlock Policies ▲

Enable lock script during locking of the user's AccessAgent session?
No

Lock script type
Batch

Lock script code

Enable unlock script when user unlocks an existing AccessAgent session?
No

Unlock script type
Batch

Unlock script code

Unlock computer policy
Any user with or without current desktop account in Wallet can unlock

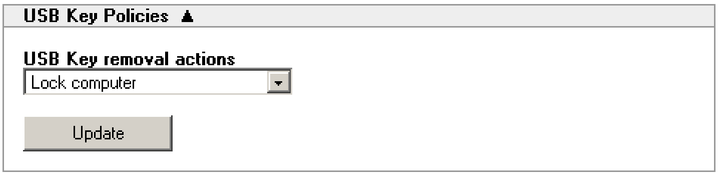
Confirmation countdown duration, in seconds, for unlocking by a different user
0

Lock/Unlock policies

Second authentication factor-related policies

Refer to this section to specify settings for second authentication factor policies.

USB Key policies



USB Key Policies ▲

USB Key removal actions
Lock computer

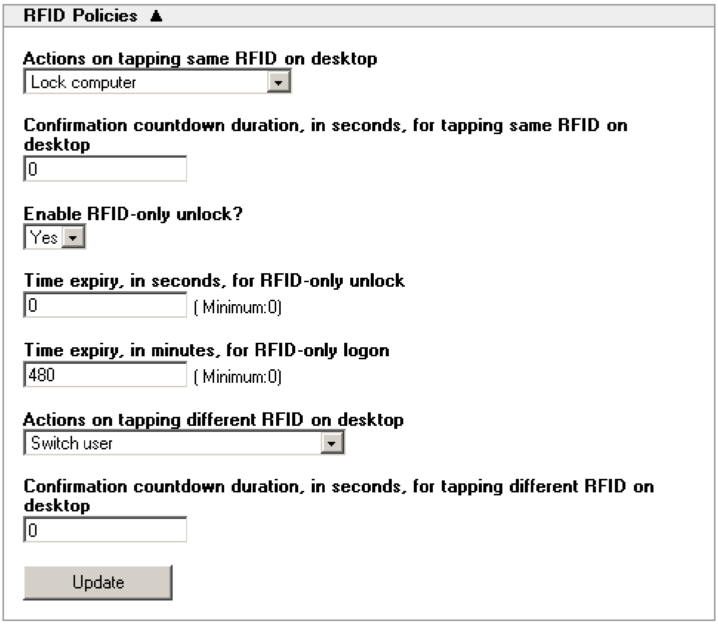
Policies when removing USB Key

USB Key removal actions

Select the action that AccessAgent will perform once the USB Key is removed from the port.

Click **Update** to confirm the changes.

RFID policies



RFID Policies ▲

Actions on tapping same RFID on desktop
Lock computer

Confirmation countdown duration, in seconds, for tapping same RFID on desktop
0

Enable RFID-only unlock?
Yes

Time expiry, in seconds, for RFID-only unlock
0 (Minimum:0)

Time expiry, in minutes, for RFID-only logon
480 (Minimum:0)

Actions on tapping different RFID on desktop
Switch user

Confirmation countdown duration, in seconds, for tapping different RFID on desktop
0

RFID policies

- Actions on tapping same RFID on desktop

  Select the action that AccessAgent performs when the logged on user taps the RFID card on the reader again.

- Confirmation countdown duration, in seconds, for tapping same RFID on desktop

  Enter the number of seconds that AccessAgent will display a message box, which appears when AccessAgent is about to perform an action after the same RFID card is tapped on the reader.

The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click Yes to proceed with the action, or No to reactivate the desktop.

- Enable RFID-only unlock?

  Select Yes if the user can unlock the RFID card within a specified duration (not requiring a password).

- Time expiry, in seconds, for RFID-only unlock

  Enter the number of seconds that AccessAgent allows RFID-only unlock (not requiring a password).

- Time expiry, in seconds, for RFID-only logon

  Enter the number of seconds that AccessAgent allows RFID-only logon (not requiring password).

- Actions on tapping different RFID on desktop

  Select the actions that AccessAgent performs when a user taps a different RFID card on the reader while another user is logged on.

- Confirmation countdown duration, in seconds, for tapping different RFID on desktop

  Enter the number of seconds that AccessAgent will display a message box, which appears when AccessAgent is about to perform an action after a user taps a different RFID card on the reader.

  The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click Yes to let AccessAgent proceed with the action, or No to reactivate the desktop.

Click Update to confirm the changes.

Fingerprint identification policies

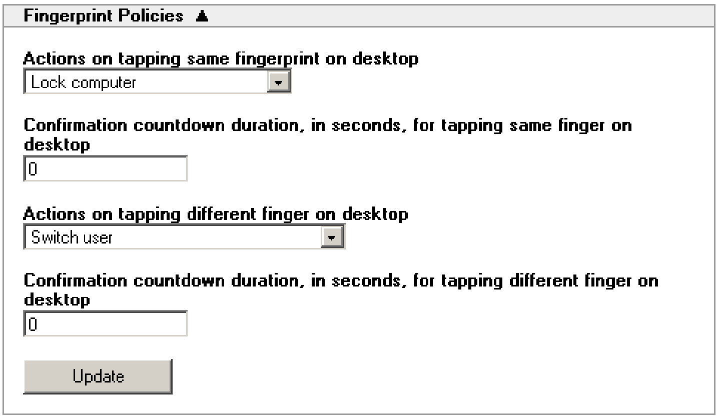
- Actions on imprinting same finger on desktop

  Select the action that AccessAgent performs when a logged on user imprints the same finger on the fingerprint reader.

- Confirmation countdown duration, in seconds, for tapping same finger on desktop

  Enter the number of seconds that AccessAgent will display a message box, which appears when AccessAgent is about to perform an action after a user imprinted the same finger on the finger print reader.

The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** to let AccessAgent proceed with the action, or **No** to reactivate the desktop.



Fingerprint Policies ▲

Actions on tapping same fingerprint on desktop: Lock computer

Confirmation countdown duration, in seconds, for tapping same finger on desktop: 0

Actions on tapping different finger on desktop: Switch user

Confirmation countdown duration, in seconds, for tapping different finger on desktop: 0

Fingerprint identification policies

- **Actions on imprinting different finger on desktop**

  Select the action that AccessAgent performs when another user imprints a finger on the reader, even though another user is logged on.

- **Confirmation countdown duration, in seconds, for tapping different finger on desktop**

  Enter the number of seconds that AccessAgent will display a message box, which appears when AccessAgent is about to perform an action after a different user imprinted a finger on the finger print reader.

  The message box provides two options for the user, one of which must be selected before the specified number of seconds expire. The user can either click **Yes** to let AccessAgent proceed with the action, or **No** to reactivate the desktop.

Click **Update** to confirm the changes.

Logon/logoff policies

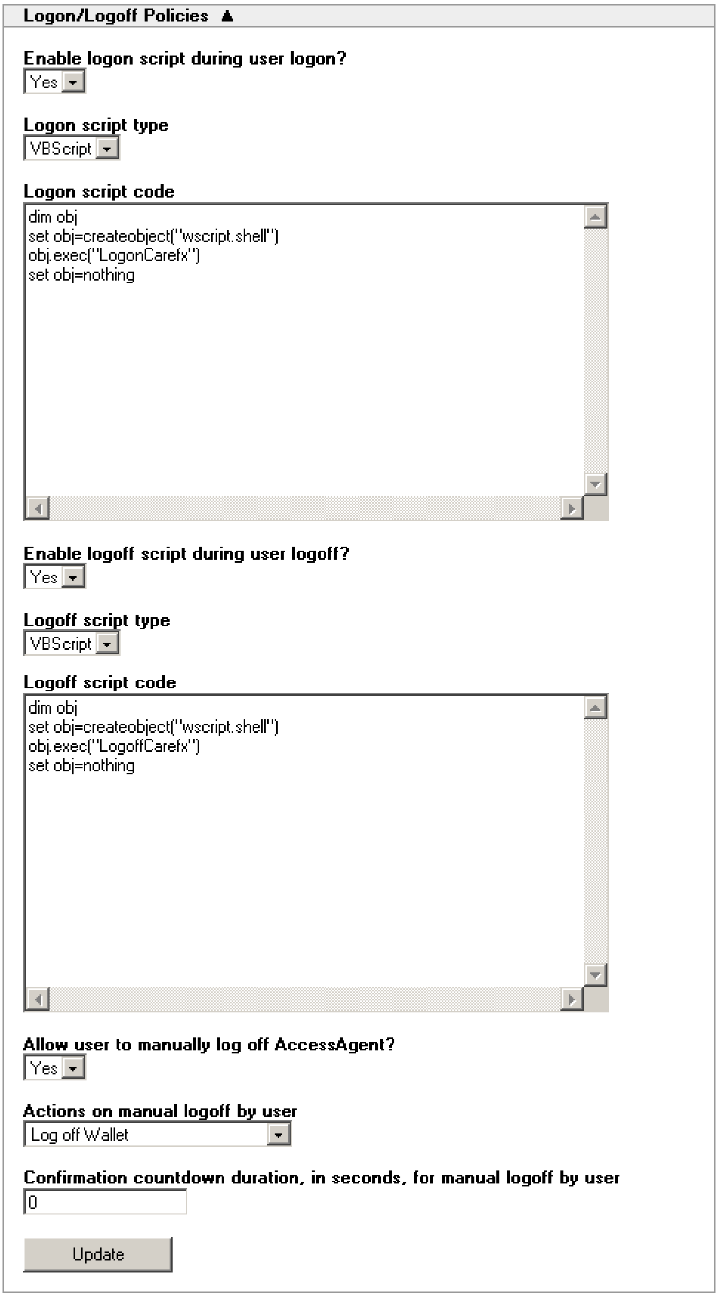
Use the logon/logoff policies to define the AccessAgent behavioral patterns when a user logs on to or logs off from AccessAgent.

- **Enable logon script during user logon?**

  Select Enabled if a script will run whenever the user logs on to AccessAgent. The logon script specifies various actions that AccessAgent will perform upon logon, such as selecting the applications to start, selecting the network resources to reconnect to, etc.

- Logon script type

  Select the types of logon script used with AccessAgent. You can either select Batch file or VB script.



Logon/Logoff Policies ▲

Enable logon script during user logon?
Yes ▾

Logon script type
VBScript ▾

Logon script code

```
dim obj
set obj=createobject("wscript.shell")
obj.exec("LogonCarefx")
set obj=nothing
```

Enable logoff script during user logoff?
Yes ▾

Logoff script type
VBScript ▾

Logoff script code

```
dim obj
set obj=createobject("wscript.shell")
obj.exec("LogoffCarefx")
set obj=nothing
```

Allow user to manually log off AccessAgent?
Yes ▾

Actions on manual logoff by user
Log off Wallet ▾

Confirmation countdown duration, in seconds, for manual logoff by user
0

Logon/logoff policies

- Logon script code

  Copy the logon script's source code in the text box.

- Enable logoff script during user logoff?

  Enable this policy to run a script whenever the user logs off from AccessAgent. The logoff script specifies various actions that AccessAgent will perform upon logoff, such as selecting the applications to close, selecting the network resources to disconnect from, etc.

- Logoff script type

  Select the types of logoff script used with AccessAgent. You can either select Batch file or VB script.

- Logoff script code

  Copy the logoff script's source code in the text box.

- Allow user to manually log off AccessAgent?

  Select Yes to allow users to log off from AccessAgent manually.

- Actions on manual logoff by user

  Select the action AccessAgent performs when the user logs off.

- Confirmation countdown duration, in seconds, for manual logoff by user

  Enter the number of seconds the computer can request the user to confirm logoff after a period of inactivity.

Click Update to confirm the changes.

Setting authentication service policies

Use the authentication service policies to set the enterprise authentication service.

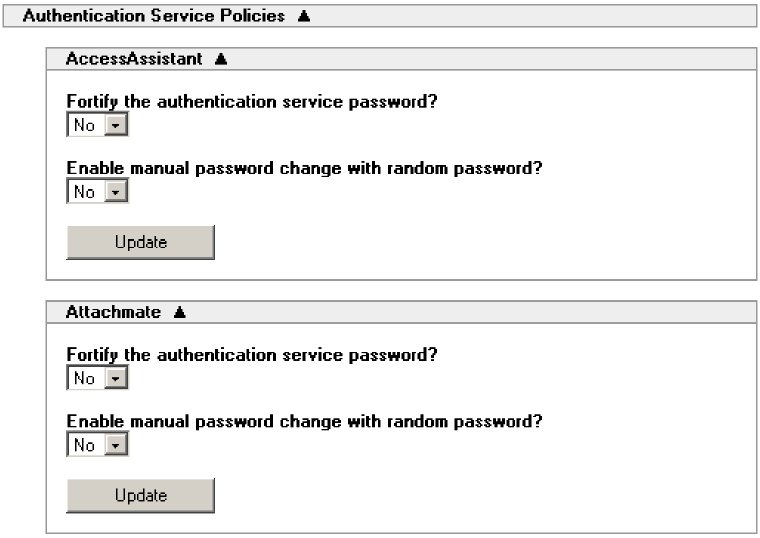
- Fortify the authentication service password?

  Select Yes to change your authentication service password with a randomly-generated password regularly.

- Enable manual password change with random password?

  Select Yes to allow AccessAgent to auto-fill a randomly generated password when a user changes the password manually.

Click Update to confirm the changes.



Authentication Service Policies ▲

AccessAssistant ▲

Fortify the authentication service password?
No

Enable manual password change with random password?
No

Attachmate ▲

Fortify the authentication service password?
No

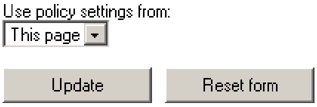
Enable manual password change with random password?
No

Authentication policies

Apply policies defined on this page

After providing the necessary changes to the policy settings, click **Update** at the bottom of the user profile page.

To cancel any changes, click **Reset form**.



Use policy settings from:
This page

Viewing system policies

This chapter discusses how to view system policies using Encentuate AccessAdmin. You can access Encentuate AccessAdmin user interface by going to: **https://hostname**, where hostname is the name of the computer where the IMS Server is installed.

The main user interface contains links to all the available administration functions. The main link, AccessAdmin, should be visible at all times. Click on the link to view the AccessAdmin user interface.

This chapter covers the following topics:

Viewing a policy template

A Helpdesk officer can only view templates, but cannot modify the templates.

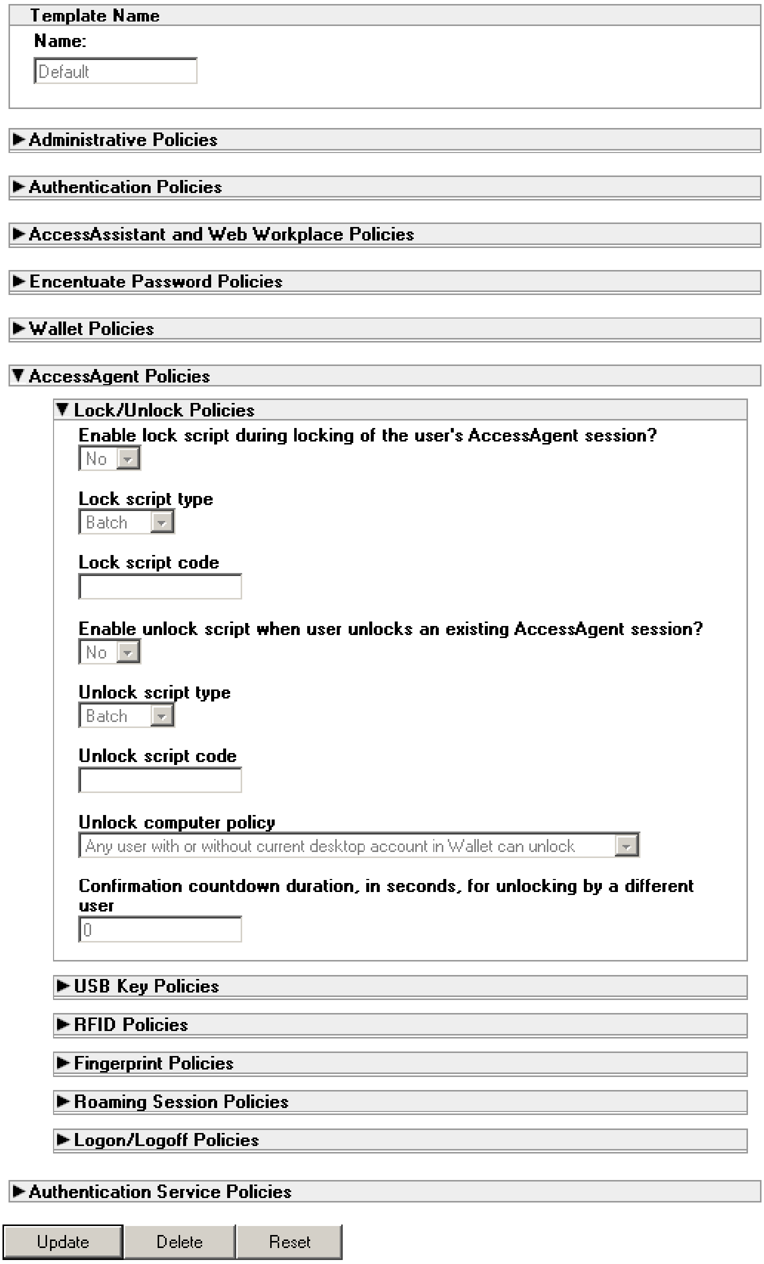
To view a policy template:

❶ In the AccessAdmin navigation panel, select *Policy Templates >> [name of template*.

There is one Default template. If the Administrator has defined any templates, these templates are displayed in the other templates available under the Policy Templates option in the navigation panel.

These other templates are fully configurable and the naming convention is set by the Administrator. Check with the Administrator to verify the details of each policy template.

❷ You can view the details of each policy by expanding the panels using the Down arrow ▼. You can also hide the details using the Up arrow ▲.



Template Name

Name: Default

▶ Administrative Policies

▶ Authentication Policies

▶ AccessAssistant and Web Workplace Policies

▶ Encentuate Password Policies

▶ Wallet Policies

▼ AccessAgent Policies

▼ Lock/Unlock Policies

Enable lock script during locking of the user's AccessAgent session? No

Lock script type: Batch

Lock script code

Enable unlock script when user unlocks an existing AccessAgent session? No

Unlock script type: Batch

Unlock script code

Unlock computer policy: Any user with or without current desktop account in Wallet can unlock

Confirmation countdown duration, in seconds, for unlocking by a different user: 0

▶ USB Key Policies

▶ RFID Policies

▶ Fingerprint Policies

▶ Roaming Session Policies

▶ Logon/Logoff Policies

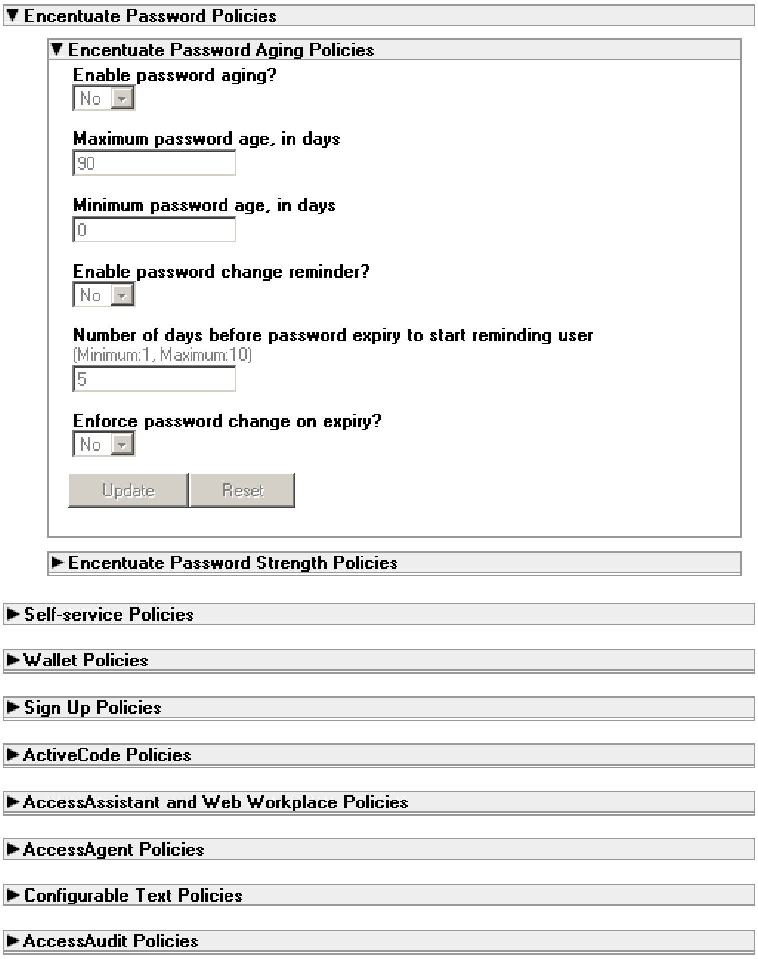
▶ Authentication Service Policies

Policy template

Viewing system policies

To view system policies:

❶ In the AccessAdmin navigation panel, select *System >> System policies.*



▼ Encentuate Password Policies

▼ Encentuate Password Aging Policies

Enable password aging?
No

Maximum password age, in days
90

Minimum password age, in days
0

Enable password change reminder?
No

Number of days before password expiry to start reminding user
(Minimum:1, Maximum:10)
5

Enforce password change on expiry?
No

▶ Encentuate Password Strength Policies

▶ Self-service Policies

▶ Wallet Policies

▶ Sign Up Policies

▶ ActiveCode Policies

▶ AccessAssistant and Web Workplace Policies

▶ AccessAgent Policies

▶ Configurable Text Policies

▶ AccessAudit Policies

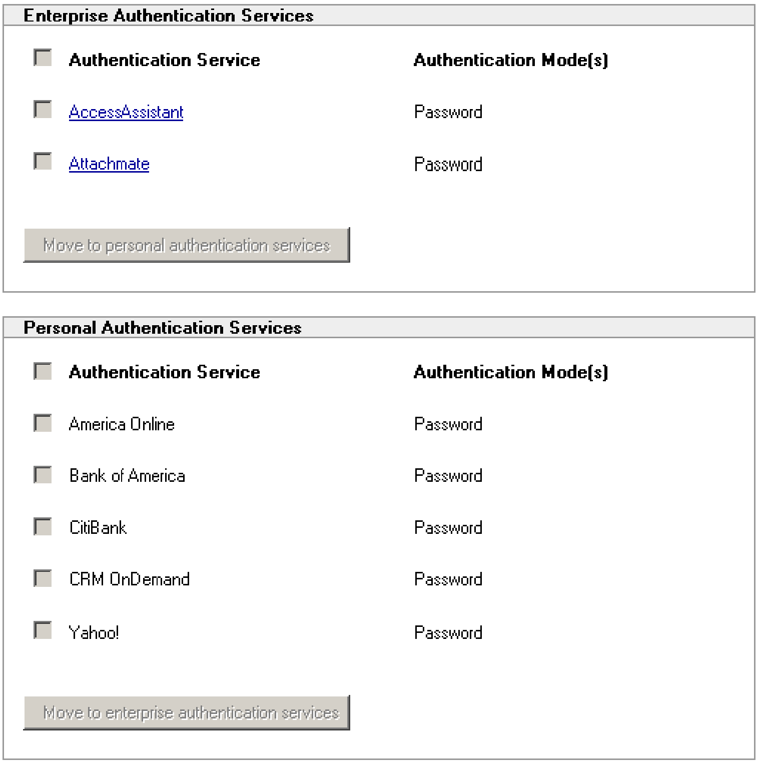
System policies

❷ You can view the details of each policy by expanding the panels using the Down arrow ▼. You can also hide the details using the Up arrow ▲.

Viewing authentication service policies

To view authentication service policies:

❶ In the AccessAdmin navigation panel, select *System >> Authentication service policies.*



Enterprise Authentication Services

□	**Authentication Service**	**Authentication Mode(s)**
□	AccessAssistant	Password
□	Attachmate	Password

Move to personal authentication services

Personal Authentication Services

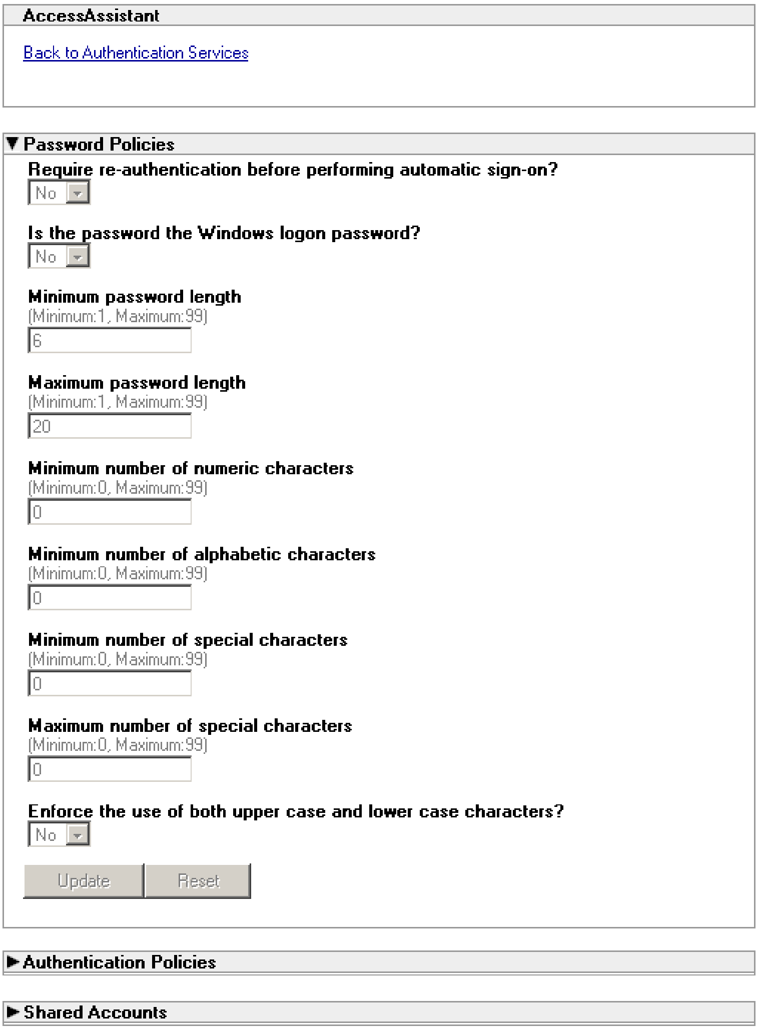
□	**Authentication Service**	**Authentication Mode(s)**
□	America Online	Password
□	Bank of America	Password
□	CitiBank	Password
□	CRM OnDemand	Password
□	Yahoo!	Password

Move to enterprise authentication services

Authentication services policies

❷ In the Enterprise Authentication Services panel, view the authentication service details by clicking on the hyperlink.

❸ You can view the details of each policy by expanding the panels using the Down arrow ▼. You can also hide the details using the Up arrow ▲.



Require re-authentication before performing automatic sign-on?
No

Is the password the Windows logon password?
No

Minimum password length
(Minimum:1, Maximum:99)
6

Maximum password length
(Minimum:1, Maximum:99)
20

Minimum number of numeric characters
(Minimum:0, Maximum:99)
0

Minimum number of alphabetic characters
(Minimum:0, Maximum:99)
0

Minimum number of special characters
(Minimum:0, Maximum:99)
0

Maximum number of special characters
(Minimum:0, Maximum:99)
0

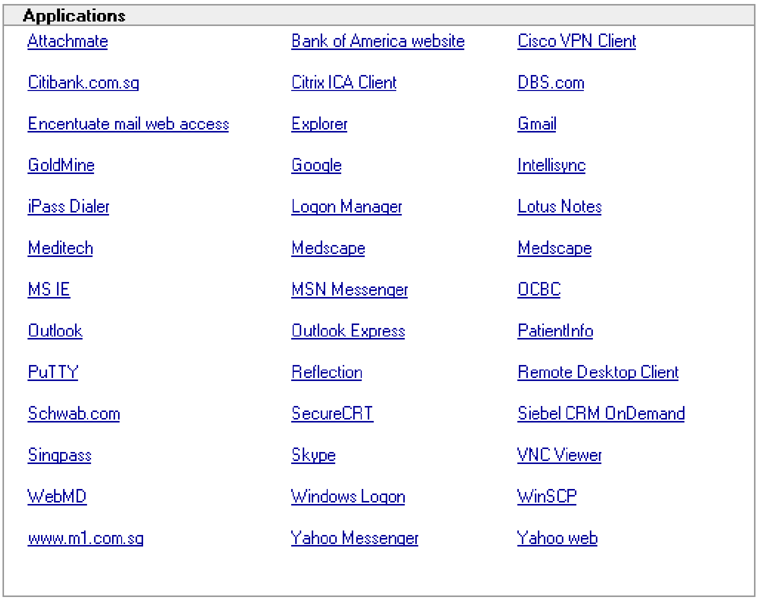
Enforce the use of both upper case and lower case characters?
No

Authentication service details

Viewing application policies

To view application policies:

❶ In the AccessAdmin navigation panel, select *System >> Application policies*.

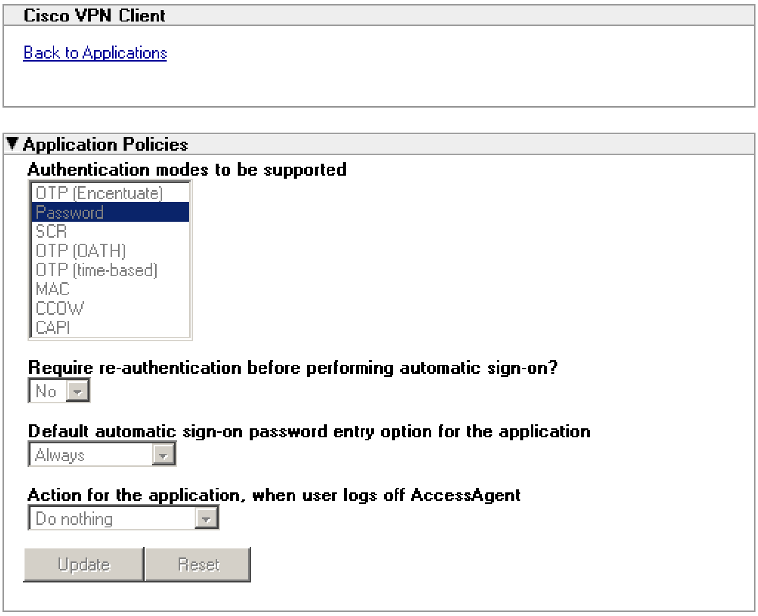


Applications

Attachmate	Bank of America website	Cisco VPN Client
Citibank.com.sg	Citrix ICA Client	DBS.com
Encentuate mail web access	Explorer	Gmail
GoldMine	Google	Intellisync
iPass Dialer	Logon Manager	Lotus Notes
Meditech	Medscape	Medscape
MS IE	MSN Messenger	OCBC
Outlook	Outlook Express	PatientInfo
PuTTY	Reflection	Remote Desktop Client
Schwab.com	SecureCRT	Siebel CRM OnDemand
Singpass	Skype	VNC Viewer
WebMD	Windows Logon	WinSCP
www.m1.com.sg	Yahoo Messenger	Yahoo web

Available applications

❷ In the Applications panel, view the details of the authentication service by clicking the hyperlink.



Cisco VPN Client

Back to Applications

▼ Application Policies

Authentication modes to be supported

OTP (Encentuate)
[✓ Password]
SCR
OTP (OATH)
OTP (time-based)
MAC
CCOW
CAPI

Require re-authentication before performing automatic sign-on?
No

Default automatic sign-on password entry option for the application
Always

Action for the application, when user logs off AccessAgent
Do nothing

Application policies

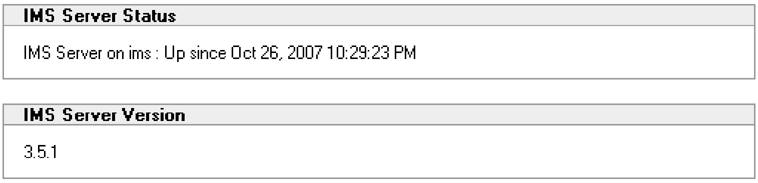
❸ You can view the details of each policy by expanding the panels using the Down arrow ▼. You can also hide the details using the Up arrow ▲.

❹ Click on **Back to Applications** to return to the previous page.

Checking IMS Server status and version

You can use AccessAdmin to view the status of the IMS server and its version number.

In the AccessAdmin navigation panel, select *System >> Status*.



IMS Server Status

IMS Server on ims : Up since Oct 26, 2007 10:29:23 PM

IMS Server Version

3.5.1

Server status and version

Sending feedback to Encentuate

To provide feedback or ask questions on the Encentuate IMS Server user interface that are not covered in this guide, click on the **Feedback** link in the AccessAdmin navigation panel.

The Feedback panel is also displayed during unexpected errors.

Entering an e-mail address is optional, which Encentuate uses update you on the progress of your feedback. Enter your comments and click **Send**.

Getting help

If you require assistance while using the Encentuate IMS Server user interface, click **Help** in the AccessAdmin navigation panel. A copy of the Encentuate IAM Helpdesk Guide is displayed. Click on a bookmark or link to navigate to a specific topic or section.

❶ Click *AccessAdmin >> About AccessAdmin >> Help*.

❷ Find the most relevant topic from the list. For more assistance, see the Encentuate IAM Administrator Guide.

Troubleshooting

The following are common user problems, their possible causes, and resolutions.

Refer to the following main troubleshooting topics:

- AccessAgent installation-related problems
- Change password-related problems
- Encentuate Wallet-related problems
- USB Key-related problems
- RFID card-related problems
- Active Proximity Badge-related problems
- Other common issues

AccessAgent installation-related problems

This section discusses problems that the user may encounter during the installation of Encentuate AccessAgent.

No Windows Administrator privileges

The user must have Windows Administrator privileges to install Encentuate AccessAgent. If you cannot provide Administrator privileges to the user, the Administrator must install Encentuate AccessAgent.

Not enough disk space

Encentuate AccessAgent will not be installed if the user's computer does not have enough free disk space. To install AccessAgent, the user must have at least 32 MB of free hard disk space. Request the user to empty the Recycle Bin, and delete unwanted files to increase free hard disk space.

Corrupt Encentuate AccessAgent installation file

If the Encentuate AccessAgent installation file was downloaded from the Internet, the download may not have completed properly. Request the user to download the file again. If the problem persists, verify if the file on the internet is corrupt, and replace the file if necessary.

Conflict with another application

If the user sees a message that says "AccessAgent's setup detected a conflict with an application and it is recommended that the application be uninstalled", the user must exit from the AccessAgent setup and uninstall the application that is causing the conflict. The user must ensure that the application is no longer being used before uninstalling the application. Once the application is uninstalled, request the user to run AccessAgent setup again.

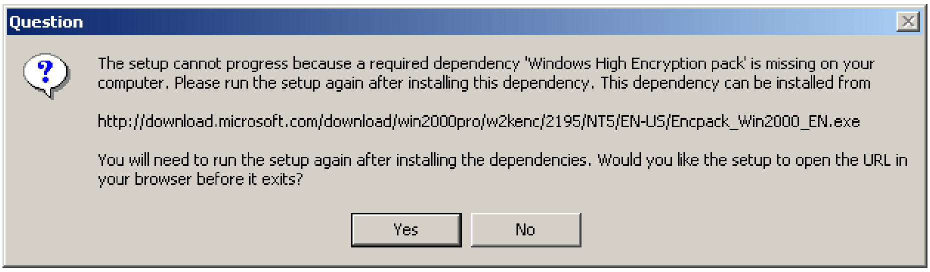
If the user ignores the prompt and continues with the installation, AccessAgent may not work properly.

A module could not be registered

If the user sees a message that says, "The system encountered a problem while registering a module (Error 1904)", the user should click **Ignore** to continue the installation. This is a documented Microsoft Windows problem and is not critical. If the problem persists, request the user to uninstall and reinstall Encentuate AccessAgent.

No encryption pack

If the user is installing AccessAgent on Windows 2000, the computer must have Enhanced Cryptographic Service Provider (CSP) installed to ensure the security of the Wallet's contents.



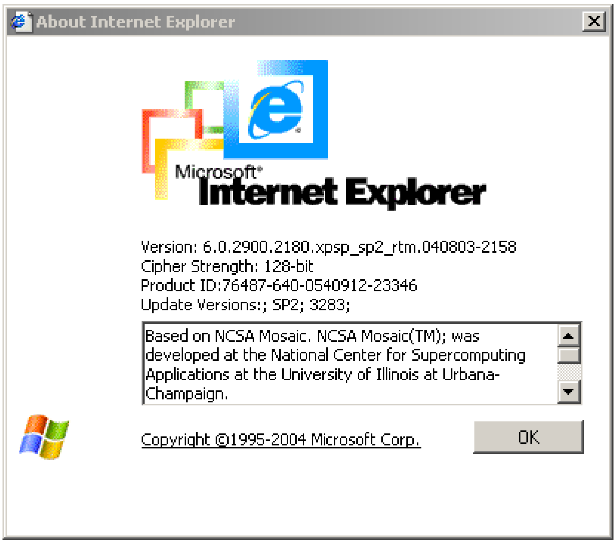
The setup cannot progress because a required dependency 'Windows High Encryption pack' is missing on your computer. Please run the setup again after installing this dependency. This dependency can be installed from

http://download.microsoft.com/download/win2000pro/w2kenc/2195/NT5/EN-US/Encpack_Win2000_EN.exe

You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?

No enhanced CSP

To check if the computer has Enhanced CSP, go to **Help >> About Internet Explorer** in Internet Explorer. If Enhanced CSP is installed it will read *Cipher Strength: 128-bit*.


About Internet Explorer

Version: 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Cipher Strength: 128-bit
Product ID:76487-640-0540912-23346
Update Versions:; SP2; 3283;

Based on NCSA Mosaic. NCSA Mosaic(TM); was developed at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.

Copyright ©1995-2004 Microsoft Corp.

Checking the cipher strength

Enhanced CSP can be downloaded from:

http://www.microsoft.com/windows2000/downloads/recommended/encryption/.

The installer cannot find IMS Server

The installer cannot locate the IMS Server if:

- The server information provided is incorrect.

  The installer tries to connect to the IMS Server automatically during the installation. If a connection is not established, the user will be asked to enter the location of the IMS Server. If the IMS Server cannot be located, a dialog box is displayed.

  Make sure that the information entered is correct and try again.

- A network connection cannot be detected.

To verify whether or not the computer has a connection to the IMS Server or network, enter the IMS Server name in your browser window. If the IMS page cannot be displayed, connection is not established.

No network connection

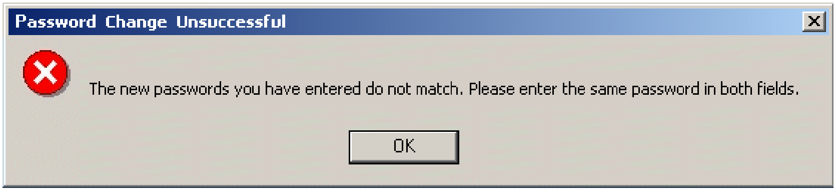
A network connection is required to install AccessAgent, to sign up, or to change the Encentuate password. If the system does not detect a network connection while installing Encentuate AccessAgent, a dialog box is displayed. Make sure that the network settings are correct and try again.

Change password-related problems

Entries do not match

If the user is trying to change a password, and the entries for Change password and Confirm password do not match, a dialog box is displayed.

Ask the user to re-enter a new password in New password and Confirm password fields.



Password Change Unsuccessful

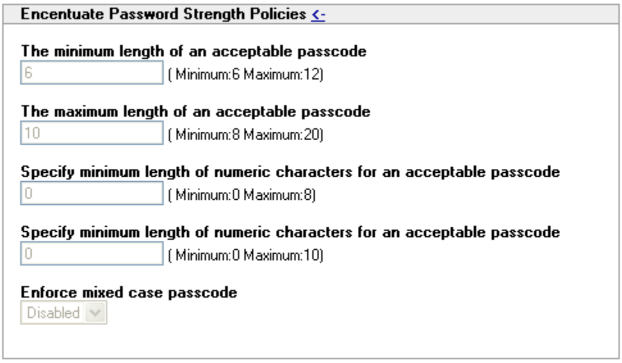
The new passwords you have entered do not match. Please enter the same password in both fields.

Password entries do not match

Incorrect password length

If the user is trying to change a password and the new password is less than the minimum number of characters, the system will prompt the user to enter a password within the required length.

The length of the password is fully configurable. The Administrator can configure the length of the password. To view the settings from Encentuate AccessAdmin, go to System >> System Policies >> Encentuate password Strength Policies.



Encentuate Password Strength Policies <-

The minimum length of an acceptable passcode
6 (Minimum:6 Maximum:12)

The maximum length of an acceptable passcode
10 (Minimum:8 Maximum:20)

Specify minimum length of numeric characters for an acceptable passcode
0 (Minimum:0 Maximum:8)

Specify minimum length of numeric characters for an acceptable passcode
0 (Minimum:0 Maximum:10)

Enforce mixed case passcode
Disabled

Password strength policies

Request the users to re-enter a new password that complies to the prescribed settings.

No network connection

If a network connection is not detected when trying to change a password, a dialog box is displayed to request the user to check the network connection and then try again.

Encentuate Wallet-related problems

Incorrect Windows user account

Before signing up for an Encentuate Wallet, the user must first enter the Windows user name and password to store these credentials in the Wallet. The user name and password are verified with Windows. If they do not match, an error message is displayed.

Request the user to check if the correct user name and password are used, if the Caps Lock key is not active, and that the characters are entered in the correct case.

Forgotten or unknown application user name and password

If the user forgets the application user name or password, the user requests Helpdesk to reset the application password, or uses AccessAssistant to view the user name and password.

Refer the user to the Encentuate IAM User Guide’s Troubleshooting section for further instructions.

Encentuate Wallet has been locked

The Encentuate Wallet will be locked after a set number of unsuccessful attempts to log on using an incorrect password. The number of allowed attempts can be configured by the Administrator.

If the user’s Wallet is locked, issue an authorization code for the user to unlock the Wallet.

If the user is using a USB Key, it cannot be used until it is reset. You also need to issue the user a new USB Key. When the user receives the new USB Key, it should be registered with the IMS server.

The locked Encentuate USB Key should be returned to Encentuate to be reset.

Forgotten password

If the user forgets the password, provide the user with an authorization code to reset it.

To reset a password, the user needs:

- an authorization code from the Helpdesk officer or Administrator
- secret
- new password

Refer the user to the Encentuate IAM User Guide’s Troubleshooting section for further instructions.

Forgotten secret

The secret is required to retrieve the user's Windows user name and password and to retrieve the contents of the Wallet. If the user cannot remember the secret, the user cannot access all the user credentials stored in the Wallet is lost. The only option is to start again by signing up for another Wallet.

Temporary Wallet's validity period has expired

If the user has been given a temporary access to the Wallet, the Wallet is only valid for a predefined time. Once the validity of the temporary Wallet expires, the user can no longer use the Wallet. Issue a new authorization code to provide the user with temporary access.

USB Key-related problems

Cannot unlock computer with USB Key

If the user is trying to unlock a computer and is prompted that the password could not be validated, request the user to remove and reinsert the USB Key from the USB port.

If the problem persists, request the user to unlock the computer using the Windows user name and password. Select Go to Windows to unlock in the navigation panel of the Unlock This Computer window.

Once unlocked using Windows, the user can now reset the password.

Lost Encentuate USB Key

If the user lost the Encentuate USB Key, provide the user with a new Encentuate USB Key and an authorization code. The authorization code is required to associate the Wallet with the new USB Key.

You can also provide the user temporary access to the Wallet, in case a new USB Key is not readily available. Providing temporary access also means you must provide an authorization code.

If the user cannot connect to the Encentuate IMS server, ask the user for a request code displayed on the user's AccessAgent reset password screen. You can then issue an authorization code for offline access, which does not require IMS Server connectivity.

Cannot log on to Wallet using USB Key

There can be several reasons why the user cannot log on using an Encentuate USB Key.

- Incorrect password.

  Request the user to re-enter the password. Check the Caps Lock key is not active and that the letters are entered in the correct case.

If the user has forgotten the password, provide an authorization code for the user to reset the password.

- Damaged or corrupted Encentuate USB Key

  The Encentuate USB Key may be damaged or corrupted. In this case, replace the USB Key with a new one, and return the damaged/corrupted USB Key to Encentuate to be analyzed.

- Unable to detect the Encentuate USB Key

  There may be a time-out while trying to access, validate or detect a USB Key. Request the user to remove and re-insert the USB Key from the USB port. If the problem persists, restart the computer.

  If the problem is not resolved, the USB Key may be damaged or corrupted. Replace the USB Key with a new one.

Cannot register an Encentuate USB Key

Incorrect Windows user account

To sign up, the user must enter the Windows user name and password to store the credentials in the Encentuate Wallet. Some installations may ask for additional information to establish identity. The user name and password are verified with Windows. If they do not match, a message is displayed.

Request the user to check that the correct user name and password are entered and that the characters are entered in the correct case.

If the problem persists, check the Windows user name to verify that the user is entering the correct user name. If the user name is correct, the password may be incorrect. Reset the password and provide the new password to the user.

USB Key is already registered

If the Encentuate USB Key is already registered with IMS Server, the user will be prompted. This means that the USB Key that was given to the user has probably been used by another user, but has not been revoked from the IMS Server. Retrieve the USB Key from the user and provide the user a new USB Key. Ask the user to register the new USB Key.

USB Key has been revoked

An Encentuate USB Key must be revoked once it is reported as lost. If the user finds the lost USB key and tries to log on, the system displays a message that the USB Key has been revoked.

A USB Key must be reset before it can be used again.

To use a revoked USB Key, issue an authorization code, and request the user to register the USB Key to associate it with the Wallet.

USB Key is write-protected

If the Encentuate USB Key is a V1 or a V3 key, the user may encounter a problem with write-protection. If the Encentuate USB Key is write-protected, the user cannot complete the registration process. If this happens, request the user to do the following:

1. Log off from the computer.

2. Remove the USB Key from the USB port, and write-enable it.

3. Insert the USB Key in the USB port and log on to the computer.

   The user will be prompted to register the USB Key again.

RFID card-related problems

Cannot unlock computer with RFID card

If the user is trying to unlock the computer and is prompted that the password could not be validated, request the user to tap the RFID card on the reader and enter the password again.

If the problem persists, request the user to unlock the computer using the Windows user name and password. Select Go to Windows to unlock in the navigation panel of the Unlock This Computer window.

Once unlocked using Windows, the user can now reset the password.

Lost Encentuate RFID card

If the user lost the Encentuate RFID card, provide the user with a new Encentuate RFID card and an authorization code. The authorization code is required to associate the Wallet with a new RFID card.

You can also provide the user temporary access to the Wallet, in case a new RFID card is not readily available. Providing temporary access also means you must provide an authorization code.

If the user cannot connect to the Encentuate IMS server, ask the user for a request code displayed on the user's AccessAgent reset password screen. You can then issue an authorization code for offline access, which does not require IMS Server connectivity.

Cannot log on to Wallet using RFID card

There can be several reasons why the user cannot log on to the Wallet.

- Incorrect password.

  Request the user to re-enter the password. Check the Caps Lock key is not active and that the letters are entered in the correct case.

If the user has forgotten the password, provide an authorization code for the user to reset the password.

- Damaged or corrupted Encentuate RFID card or reader

  If the Encentuate RFID card or reader is damaged or corrupted, you will need to replace it.

- Unable to detect the Encentuate RFID card

  There may be a time-out while trying to detect your RFID card. Request the user to tap the RFID card on the reader once again. If the problem persists, request the user to restart the computer.

  If the problem is not resolved, the RFID card may be damaged or corrupted. Replace the RFID card with a new one.

Cannot register an RFID card

RFID card is already registered

If the user tries to register an Encentuate RFID card that has already been registered with IMS Server, a message is displayed. That the RFID card has probably been used by another user, but has not been revoked from the IMS Server. Request the user to return the RFID card and replace it with a new RFID card.

RFID card has been revoked

An RFID card must be revoked once it is reported as lost. If the user finds the lost RFID card and tries to log on, the system will display a message that the RFID card has been revoked.

To use a revoked RFID card, issue an authorization code, and then request the user to register the revoked RFID card again to associate it with the Wallet.

Active Proximity Badge-related problems

This section discusses problems that relate to an Encentuate Active Proximity Badge and reader.

Cannot unlock computer with Active Proximity Badge

If the user is trying to unlock the computer and is prompted that the password could not be validated, request the user to switch the Active Proximity Badge off and then on, and select it from the list. When prompted, enter the password again.

If the problem persists, request the user to unlock the computer using the Windows user name and password. Select Go to Windows to unlock in the navigation panel of the Unlock This Computer window.

After logging on through Windows, the user can now reset the password.

Lost Encentuate Active Proximity Badge

If the user lost the Encentuate Active Proximity Badge, provide the user with a new badge and an authorization code. The authorization code is required to associate the Wallet with a new Active Proximity Badge.

You can also provide the user temporary access to the Wallet, in case a new USB Key is not readily available. Providing temporary access also means you must provide an authorization code.

If the user cannot connect to the Encentuate IMS server, ask the user for a request code displayed on the user's AccessAgent reset password screen. You can then issue an authorization code for offline access, which does not require IMS Server connectivity.

Cannot log on to Wallet

There can be several reasons why the user cannot log on to the Wallet.

- Incorrect password.

  Request the user to re-enter the password. Check the Caps Lock key is not active and that the letters are entered in the correct case.

  If the user has forgotten the password, provide an authorization code for the user to reset the password.

- Damaged or corrupted Encentuate Active Proximity Badge or reader

  If the Encentuate Active Proximity Badge is damaged or corrupted, replace it with a new badge.

- Unable to detect the Encentuate Active Proximity Badge

  There may be a time-out while trying to detect the Active Proximity Badge, or the card has been switched on for nine hours—after which it automatically switches off. Request the user to switch the badge off and on. If the problem persists, restart the computer.

  A substantial reduction on battery power may also be the reason why the Active Proximity Badge cannot be detected. In this case, replace the battery.

  If the problem is not resolved, the Encentuate Active Proximity Badge may be damaged or corrupted. Replace the Encentuate Active Proximity Badge with a new one.

Cannot register an Active Proximity Badge

Active Proximity Badge is already registered

If an Encentuate Active Proximity Badge is already registered with the IMS Server, a message is displayed. The Active Proximity Badge has probably been used by another user, but has not been revoked from the IMS Server. Retrieve the Active Proximity Badge from the user, and issue a new Active Proximity Badge.

Active Proximity Card has been revoked

An Active Proximity Badge must be revoked once it is reported as lost. If the user finds the lost Active Proximity Badge and tries to log on, a message is displayed that Active Proximity Badge has been revoked.

To use a revoked Active Proximity Badge, issue an authorization code, and then request the user to register the new Active Proximity Badge again to associate it with the Wallet.

Cannot detect Active Proximity Badge

The incorrect placement of the reader and badge can affect the signal. The reader and badge should be at the same level, if the reader is mounted on the monitor, the badge should be placed on the upper part of the body.

Distance is not an issue. Some elements may affect the radio frequency signal, such as the desk, body, keyboard, etc. Even the user's arm passing in front of the reader can cause the signal to drop slightly.

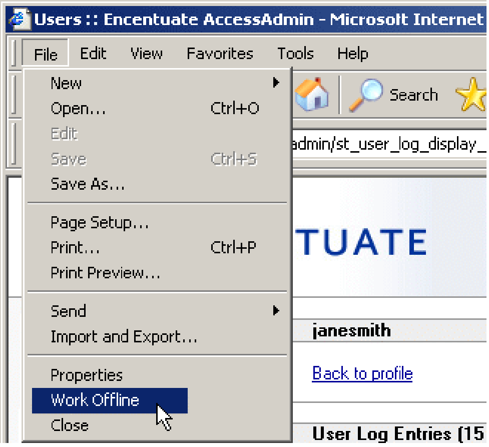
You can review the badge positioning demo at the following URL:

http://www.ensuretech.com/support/documentation/movies/lockpositionlowres.mpg/.

Other common issues

Internet Explorer is set to offline

If the user sees a network connection-related message, Internet Explorer may be set to offline mode. You can check this by going to the File menu in Internet Explorer and check that the Work Offline option is not selected.



Internet Explorer set to online

System does not accept authorization code

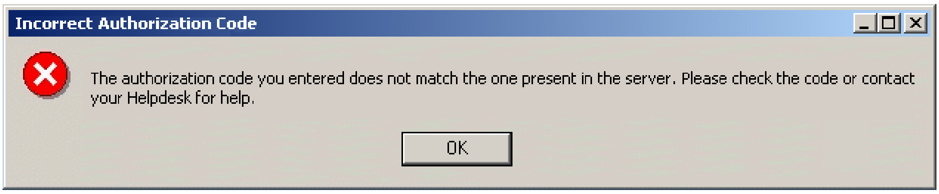
An authorization code is provided by a Helpdesk officer to allow the user to use AccessAssistant, to temporarily log on to AccessAgent without a second authentication factor, or to reset a password. If the system does not accept the user's authorization code, it could be because:

- The user did not enter the correct authorization code.

  Request the user to make sure that the characters are entered in the correct order.

- The user does not have the correct authorization code.

  An incorrect authorization code may have been communicated to the user, or it may be incomplete (some characters missing). Depending the authorization code validity, provide the user a new authorization code.



The authorization code you entered does not match the one present in the server. Please check the code or contact your Helpdesk for help.

Wrong authorization code

System does not accept password

If the user reports that the system does not accept a password, the user may not be entering the correct password, or the user may be not be entering the password in the correct case.

Request the users to check that the Caps Lock key is not active, and that letters are entered in the correct case.

If the user has forgotten the password, give the user an authorization code to reset the password. After providing the authorization code, you can refer the user to the Encentuate IAM User Guide's Troubleshooting section for further instructions.

System does not accept secret

If the user reports that the system does not accept a secret, the user may not be entering the correct secret. Request the user to enter the secret again. If the problem persists, request the user to sign up for a new Wallet.

Index